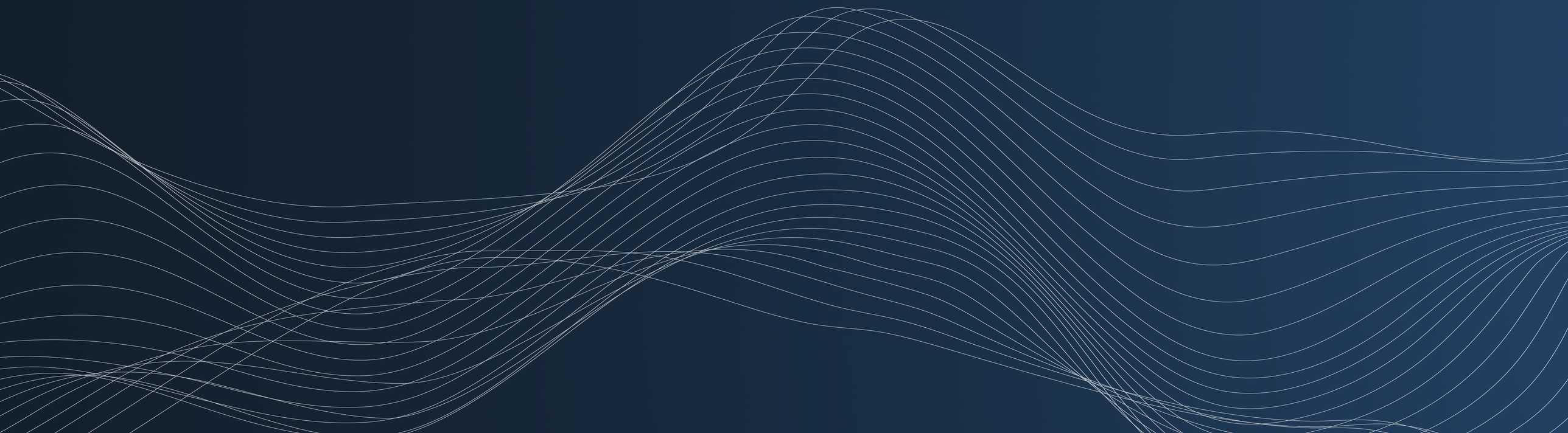
Québec

Bureau du scientifique en chef du Québec

Naviguer dans les désordres de l'information

Un guide sur la mésinformation, la désinformation et la malinformation pour les titulaires de charge publique du Québec



Naviguer dans
les désordres
de l’information

Bureau du scientifique en chef du Québec
Fonds de recherche du Québec (FRQ)
500, rue Sherbrooke Ouest, bureau 800
Montréal (Québec) H3A 3C6
www.scientifique-en-chef.gouv.qc.ca

Recherche et rédaction
Julie Dirwimmer, conseillère stratégique - relations sciences et société, FRQ
Émilie Michaud, stagiaire, FRQ

Coordination
Julie Dirwimmer, conseillère stratégique - relations sciences et société, FRQ
Véronique Sauriol, conseillère aux communications, FRQ

Révision linguistique
Isabelle Gandilhon

Graphisme et mise en page
Macadam

Date de publication
Octobre 2025

ISBN : 978-2-555-02388-8

MOT DU SCIENTIFIQUE EN CHEF 04

INTRODUCTION 05

À QUI S'ADRESSE CE GUIDE? 07

COMMENT CE GUIDE A-T-IL ÉTÉ CONÇU? 07

LES DÉSORDRES DE L'INFORMATION : UN PORTRAIT DU PHÉNOMÈNE 08

UNE TYPOLOGIE DES DÉSORDRES DE L'INFORMATION 09

UN CONTEXTE PROPICE À L'AMPLIFICATION DES DÉSORDRES INFORMATIONNELS 12

CARACTÉRISTIQUES DU PHÉNOMÈNE AU QUÉBEC 14

LES EFFETS SUR LES ADMINISTRATIONS PUBLIQUES ET LA DÉMOCRATIE 18

AUGMENTEZ VOTRE DISCERNEMENT INDIVIDUEL 19

FICHE 1 QUELQUES TECHNIQUES POUR TROMPER LES INTERNAUTES 20

FICHE 2 MÉFIEZ-VOUS DE VOS ÉMOTIONS 22

FICHE 3 LES DÉFAUTS DE VOTRE CERVEAU : LES BIAIS COGNITIFS 23

FICHE 4 LES DÉFAUTS DE VOTRE CERVEAU : LES SOPHISMES 24

FICHE 5 CETTE NOUVELLE SUR LE WEB EST-ELLE FIABLE? 26

FICHE 6 CONFIRMEZ LA VÉRACITÉ D'UNE IMAGE OU D'UNE VIDÉO 28

FICHE 7 RÉDUISEZ VOTRE DÉPENDANCE AUX ALGORITHMES 30

FICHE 8 ÉVALUEZ LA VALEUR D'UNE INFORMATION SCIENTIFIQUE 31

FICHE 9 COMMENT SE PORTE VOTRE EMPREINTE NUMÉRIQUE? 33

AUGMENTEZ VOTRE DISCERNEMENT INSTITUTIONNEL 35

QUELQUES PRINCIPES DE COMMUNICATION PUBLIQUE 36

ACTIONS PROACTIVES 38

FICHE 10 VEILLE CIBLÉE : DÉPLOYEZ VOS ANTENNES 39

FICHE 11 ÉVALUEZ LES RISQUES D'OPÉRATIONS D'INFLUENCE 41

FICHE 12 CONFIGUREZ LES MÉDIAS SOCIAUX 43

FICHE 13 ANIMEZ LES ESPACES DE DIALOGUE 45

FICHE 14 MIEUX VAUT PRÉVENIR QUE GUÉRIR… L'INOCULATION 47

FICHE 15 UTILISATION RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE 49

FICHE 16 CONTRIBUEZ À UN CLIMAT SAIN DANS LES DÉBATS PUBLICS 51

ACTIONS RÉACTIVES 52

FICHE 17 FACE À LA CRISE : ANALYSEZ LA SITUATION 53

FICHE 18 FACE À LA CRISE : QUELQUES BALISES POUR VOTRE PLAN D'ACTION 55

FICHE 19 DÉMYSTIFICATION ET RÉTABLISSEMENT DE FAITS 57

FICHE 20 LEVIERS JURIDIQUES RELIÉS AUX DÉSORDRES DE L'INFORMATION 59

FICHE 21 ACTIONS EN JUSTICE : COMMENT PROCÉDER? 61

CONCLUSION 63

POUR ALLER PLUS LOIN 65

RÉFÉRENCES 69

ANNEXE COMITÉ ÉDITORIAL ET PERSONNES CONSULTÉES 75

Mot de Rémi Quirion
Scientifique en chef du Québec

Pas facile de garder le cap, quand on navigue dans les désordres de l'information. Les interactions dans les arènes politiques se sont transformées, nous rappelant que la démocratie ne devrait jamais être considérée comme un acquis. Les esprits s'échauffent dans les conseils municipaux, les opérations d'influence étrangère se multiplient pendant les périodes électorales, et il devient de plus en plus difficile pour quiconque de distinguer le vrai du faux. Ici et là, des personnes élues font l'impasse sur les processus démocratiques, normalisant des pratiques qui minent la confiance des populations envers leurs représentantes et représentants.

Collectivement, nous cherchons de nouvelles manière de débattre, interroger, contester, dans le respect des personnes et des libertés de chacun et chacune. Et en tant que titulaires de charge publique, nous tentons d'aiguiser notre vigilance, de ne pas perdre de vue les informations probantes.

Ce défi est collectif, et la communauté de recherche répondra présente pour nous accompagner dans ces changements. Les chercheurs et les chercheuses comprennent de mieux en mieux les désordres de l'information dans leurs spécificités locales. Au Fonds de recherche du Québec (FRQ), nous en avons fait une priorité, via la Stratégie québécoise de recherche et d'investissement en innovation (SQRI[2]). Nous soutenons les expertises académiques en matière d'usage responsable de l'IA, de cybersécurité, de citoyenneté numérique, de médias, de prévention de la radicalisation. Nous encourageons aussi la diffusion d'informations scientifiques de qualité dans les médias sociaux, notamment grâce aux bourses Dialogue et au Détecteur de rumeurs de l'Agence Science-Presse. Et nous poursuivons notre engagement aujourd'hui avec ce guide, que nous avons produit avec le soutien d'un comité éditorial composé de membres issus tant du milieu académique que des administrations publiques. Je les remercie pour leur générosité. Au fil des échanges ils ont su trouver les langages communs pour associer les connaissances scientifiques et opérationnelles, au profit de la pertinence.

Vous trouverez dans ce guide une foule d'outils et de connaissances sur plusieurs dimensions des désordres de l'information. Il ne constitue qu'un point de départ à notre travail commun. Sa diffusion sera renforcée par des rencontres avec des spécialistes et des ressources complémentaires pour que vous puissiez faire le pas supplémentaire qui fera toute la différence.

En vous souhaitant une excellente lecture.

Introduction

Les mensonges et les demi-vérités ont toujours existé[1] : les fausses rumeurs, les découvertes scientifiques soi-disant révolutionnaires, les omissions, les raccourcis idéologiques font partie, en quelque sorte, du paysage social et démocratique. Cependant, aujourd'hui tout cela semble s'amplifier dans un tourbillon de changements : les canaux d'information se multiplient, les technologies se développent à un rythme effréné, et les opinions se polarisent sur l'échiquier géopolitique[2]. La situation semble échapper collectivement à notre contrôle.

La formidable révolution numérique que nous vivons décuple de bien des façons nos performances collectives. D'un côté, toutes et tous bénéficient des médias sociaux et de l'intelligence artificielle (IA) pour dynamiser les communications corporatives, mobiliser l'information en temps record et participer plus directement au débat public. D'un autre côté, les changements sociétaux qui en découlent génèrent des déséquilibres globaux : fracture numérique, chambres d'écho, sous-représentation de groupes[1]. Nous tentons quotidiennement de poser les bons gestes dans cette sphère informationnelle transformée par les intérêts privés et idéologiques. Quelle est notre responsabilité en tant que citoyens, employeuses, parents, consommatrices, employés?

Dans les faits, tout le monde joue un rôle actif dans la chaîne de transmission de l'information. Chaque action sur les plateformes numériques, si modeste soit-elle (lire, s'abonner, partager, commenter), peut contribuer à modérer, ou à amplifier les désordres de l'information. En tant que titulaires de charge publique, vous avez, vous aussi, un impact. Les Québécoises et les Québécois comptent sur les institutions auxquelles vous contribuez pour garantir leur sécurité, pour les accompagner de manière équitable et pour prendre des décisions informées par des données probantes. À votre échelle, vous servez le bien commun et **vous portez une responsabilité partagée, avec la population et les autres institutions, de renforcer la résilience collective face aux désordres de l'information.**

Introduction

Alors, comment réaliser au mieux votre mission de service public, dans ce nouveau contexte, qui comprend une grande part d'incertitude[3]? C'est **l'intention de ce guide : renforcer votre discernement individuel et organisationnel, et proposer des outils pour que vous puissiez passer à l'action.**

Les désordres de l'information s'immiscent dans plusieurs de vos sphères d'activité et commandent des réponses multiples[3]. C'est pourquoi ce guide adopte plusieurs dimensions connexes aux désordres de l'information, dans le but de mieux les appréhender : dimensions scientifiques, juridiques, relations publiques, communications, cybersécurité, et technologies de l'information.

Par ailleurs, il est évident que, au-delà des gestes individuels et institutionnels, des actions ambitieuses pourraient être posées à l'échelle gouvernementale et internationale, pour réglementer les espaces numériques et certaines nouvelles technologies, et pour renforcer la littératie numérique et scientifique des populations. Ce n'est pas le sujet de ce guide, qui se concentre sur les actions que vous pouvez poser, dans le cadre de vos attributions.

Vous êtes aux commandes!

Ce guide a une valeur informative, et non directive. Il offre des balises pour vous orienter dans les désordres de l'information, mais c'est vous et votre institution qui choisissez la route. Les instructions formulées par votre organisation prévalent toujours sur les propositions formulées dans ce document.

Introduction

À qui s'adresse ce guide?

Ce guide s'adresse à l'ensemble des **titulaires de charge publique au Québec, actifs et actives au sein de l'État québécois et des municipalités**[4]. Il adopte une approche intégrée des réalités de la sphère politique et de la sphère administrative, car, face aux désordres de l'information, votre engagement à travailler sur la base d'informations scientifiques et pour le bien commun des Québécoises et des Québécois vous rassemble.

Dans ce guide, vous trouverez des contenus :

Pour les membres de la sphère administrative | ADMINISTRATION

Par exemple : des membres professionnels, gestionnaires ou fonctionnaires de rang élevé

Pour les membres de la sphère politique | POLITIQUE

Par exemple : des personnes élues, des membres du personnel politique

Comment ce guide a-t-il été conçu?

Ce document a été conçu par le bureau du scientifique en chef du Québec, avec le soutien d'un comité éditorial réunissant des personnes issues du milieu scientifique et des administrations publiques (voir Annexe). Il fait référence à plusieurs guides et rapports produits dans d'autres pays [3, 5, 6, 7] ou par des organisations internationales[2], tout en prenant en compte les réalités propres au Québec.

Il est organisé de telle sorte que vous puissiez consulter ses parties indépendamment, et faire circuler les fiches qui le constituent dans vos organisations. Il comprend aussi de nombreuses références faciles d'approche pour aller plus loin (voir la section 5).

Section 1
Les désordres de l’information : un portrait du phénomène

Les désordres de l'information : un portrait du phénomène

Une typologie des désordres de l'information

Les désordres de l'information comprennent l'ensemble des phénomènes qui mènent à la circulation d'informations trompeuses. Cette vision élargie mènera vos réflexions au-delà du concept de « fausses nouvelles » (*fake news*) parfois trop étriqué[3]. Tout au long de ce guide, nous vous inciterons à appréhender les désordres de l'information, non pas seulement par le type d'information qu'ils génèrent, mais aussi par la façon dont cette information a été produite, pour quelles raisons, auprès de quel public, etc[2].

Dans les faits, ces phénomènes se déploient à une vitesse si rapide et de manière si organique que vous ne pouvez pas en déterminer tous les éléments constitutifs[2]. Dans certains cas, il est difficile de faire la distinction entre les opérations d'influence et les opérations de relation publique[8], les messages erronés disparaissent puis refont surface, la source n'est pas identifiable ou l'est difficilement, du fait de l'IA générative… **Dans cet univers d'incertitude, vous devriez vous concentrer, avant tout, à limiter les effets de ces phénomènes sur vos publics cibles et sur votre mission, plutôt que de chercher à en décoder toutes les dimensions.**

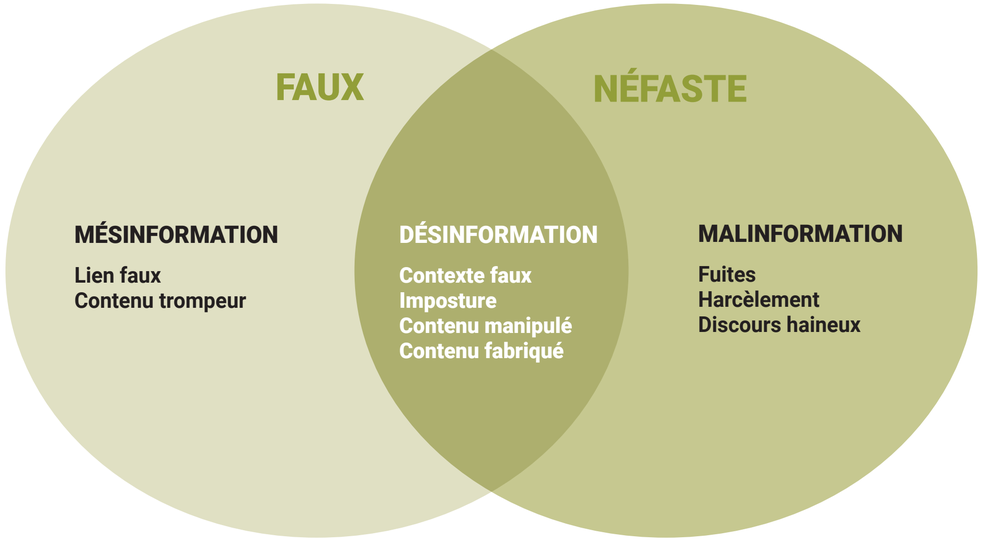
Trois postures clés pour naviguer dans les désordres de l'information

- **L'humilité.** Il est impossible de tout connaître sur tous les sujets, et encore plus de maîtriser tous les paramètres du débat public. Vous n'êtes pas seules et seuls face à ces phénomènes! Vous pouvez consulter vos collègues, et des spécialistes.
- **La nuance.** Tentez d'aller au-delà des binarités selon lesquelles il y aurait de la fausse information d'un côté, et de la vraie information de l'autre[2, 5]. Cette dichotomie contribue à accentuer les polarisations, et peut aussi mener à de la censure ou à décrédibiliser certaines parties dans les débats publics[3].
- **Le jugement.** Dans les désordres de l'information, vous devrez exercer votre jugement dans des situations ambiguës. Parfois, la ligne est mince entre une opinion critique, un exposé mal informé, un discours stratégique, ou une intention malveillante[9].

Les désordres de l'information : un portrait du phénomène

Quoi et pourquoi – qualifier les types d'informations erronées[2]

- **La mésinformation.** De l'information fausse, partagée sans intention de nuire.
- **La désinformation.** De l'information fausse, partagée volontairement, dans l'intention de causer du tort ou de manipuler délibérément les personnes.
- **La malinformation.** De l'information authentique, mais partielle, sortie de son contexte ou privée, partagée dans le but de manipuler ou de causer du tort.



Qui et comment – Comprendre les éléments constitutifs du phénomène[2]

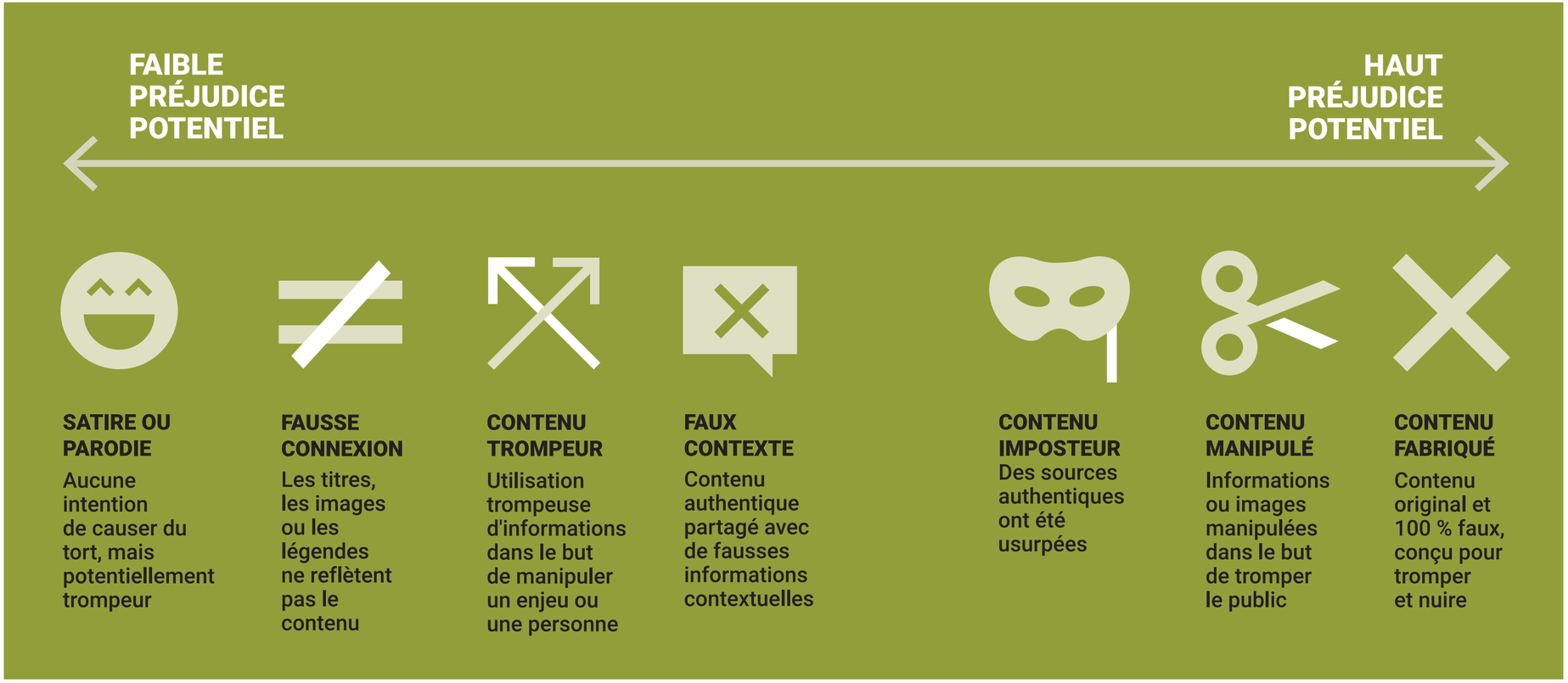
AGENT	Type d'acteur et d'actrice	Officiel / non officiel
	Niveau d'organisation	Aucune / souple / rigide / en réseau
	Type de motivation	Financière / politique / sociale / psychologique
	Niveau d'automatisation	Humaine / cyborg / robot
	Public visé	Membre / groupe social / société complète
	Volonté de nuire	Oui / non
	Volonté d'induire en erreur	Oui / non
MESSAGE	Durée	Long terme / court terme / contextuel
	Précision	Induit en erreur / manipulé / fabriqué
	Légalité	Légal / illégal
	Type d'imposture	Aucune / image de marque / individuelle
	Cible du message	Individu / organisation / groupe social / société complète
INTERPRÈTE	Lecture du message	Hégémonique / oppositionnel / négociée
	Action menée	Ignoré / partagé en soutien / partagé en opposition

Quand – Examiner les phases du phénomène[2]

Traduction : FRQ. Les autrices remercient Claire Wardle[2] pour son aimable autorisation.

Les désordres de l'information : un portrait du phénomène

Sept types courants de désordres de l'information[2]



Les désordres de l'information : un portrait du phénomène

Un contexte propice à l'amplification des désordres informationnels

L'amplification actuelle des désordres de l'information et de leurs effets s'ancre dans la conjonction de trois phénomènes : la mutation de la sphère médiatique, l'utilisation de l'intelligence artificielle et les transformations géopolitiques.

Au tournant des années 2000, le rapport de la population à l'information a complètement changé. L'apparition des médias sociaux a constitué une véritable révolution numérique. Ils ont facilité les interconnexions entre les gens et l'accès aux contenus scientifiques, mais les algorithmes opaques et changeants de certains géants du Web ont aussi favorisé la diffusion de contenus de moins bonne qualité, avec une rapidité et une portée sans précédent[1]. Dans la même période, des médias alternatifs se sont déployés sur les plateformes numériques, avec des approches plus polarisées et des pratiques ne respectant pas toujours les normes journalistiques.

De plus, **dans les dernières années, les technologies basées sur l'IA générative ont rendu possible la fabrication de contenus trompeurs de plus en plus réalistes et adaptés aux publics**[9]. Combinés avec les algorithmes de diffusion des médias sociaux, elles constituent un outil très puissant pour amplifier artificiellement des mouvements sociaux et des idéologies[12]. Elles opèrent un changement d'échelle en permettant de publier de manière coordonnée des contenus trompeurs sur plusieurs

Médias et numérique… De quoi parle-t-on?

Dans ce guide :

- **Les médias d'information** incluent la presse écrite imprimée ou en ligne, la télévision et la radio, au niveau local ou national, respectant des normes et pratiques journalistiques.
- **Les médias sociaux** permettent aux internautes et aux institutions de créer du contenu, de le partager, de l'organiser, de le modifier et de le commenter[10, 11]. Ils regroupent notamment les plateformes de réseaux sociaux (Facebook, LinkedIn, VKontakte), de partage de photos ou de vidéos (YouTube, TikTok, Odyssee), de microblogage et de blogage (WordPress, X, TruthSocial), et les projets collaboratifs (Wikipédia).
- **Les plateformes numériques** comprennent tous les outils numériques, qu'ils génèrent des informations publiques ou non, comme les médias sociaux, les sites Web, les programmes d'intelligence artificielle générative (ChatGPT, Claude), ou les applications de discussions (Messenger, Snapchat).

Les désordres de l'information : un portrait du phénomène

plateformes et dans plusieurs régions du monde[13]. Les Québécoises et les Québécois ont adopté ces outils très rapidement, surtout les plus jeunes et les personnes à plus hauts revenus, ce qui pourrait creuser les fractures numériques déjà existantes, et générer des craintes vis-à-vis de la protection des renseignements personnels[14]. Les administrations publiques, quant à elles, se trouvent à la croisée des chemins : elles intègrent des outils d'IA pour renforcer leur efficacité, mais elles courent aussi le risque de créer des vulnérabilités[15]. En effet, **les entreprises d'IA ont rarement conçu leurs produits sur la base des mêmes principes éthiques que ceux des administrations publiques (transparence, reproductibilité, etc.)**.

Par ailleurs, tous les États n'ont pas les mêmes intérêts vis-à-vis des plateformes numériques, ce qui rend la réglementation de ces dernières difficile. Les rapports de force dans le monde se dessinent de plus en plus autour de la maîtrise des technologies de l'information[13], dans une forme de course au cyberarmement[12]. La désinformation en ligne fait désormais partie de l'arsenal offensif de certains États. Ils peuvent développer des médias sociaux favorables à leur idéologie, utiliser l'intelligence artificielle pour générer des conversations polarisantes dans le but de déstabiliser les démocraties, en particulier pendant les périodes électorales[16]. De plus, certains États démocratiques comme le Canada, qui collaboraient auparavant ouvertement avec les États-Unis pour déployer des stratégies défensives, voient leurs alliances naturelles remises en question du fait des nouvelles politiques américaines.

Les polarisations en ligne se transposent hors-ligne[17]

L'assaut du Capitole des États-Unis, survenu le 6 janvier 2021, a démontré de manière flagrante comment la désinformation hors-ligne et en ligne pouvait alimenter les polarisations et mener à des actes violents, affectant les piliers mêmes des institutions démocratiques.

Les désordres de l'information : un portrait du phénomène

Caractéristiques du phénomène au Québec

S'il est difficile de mesurer précisément l'ampleur des désordres de l'information au Québec, on peut affirmer qu'ils sont bel et bien présents, et en montrer certaines spécificités.

Les désordres de l'information se manifestent, entre autres, dans le contexte de crises; Les peurs et les incertitudes favorisent la diffusion et l'adhésion rapide à toutes sortes d'informations : rumeurs, discours haineux, discours conspirationniste, etc.[18] Par exemple, les contenus liés à la désinformation climatique tendent à augmenter lors d'événements climatiques extrêmes ou lors de rencontres internationales comme les Conférences des parties (COP), qui donnent l'occasion à certains créateurs et créatrices de contenu d'inscrire le déni climatique dans le programme politique du Québec[20]. Ce mouvement contribuerait à entretenir une relation ambivalente de la population avec les changements climatiques[19]. Il se base en partie sur une remise en question du consensus scientifique, notamment de la fiabilité des mesures et des signes tangibles des changements climatiques (comme les événements météorologiques extrêmes)[20].

Dans le même ordre d'idée, la pandémie de COVID-19 a constitué un point tournant en matière de désordres de l'information[18] et a entraîné des effets très concrets : un rapport du Conseil des académies canadiennes estime que l'hésitation vaccinale alimentée par les désordres de l'information aurait généré 2 800 décès et 13 000 hospitalisations supplémentaires pendant la première vague[21]. Si la pandémie a permis à certains scientifiques de devenir des personnalités publiques, elle a aussi permis à des personnes relayant du contenu trompeur ou conspirationniste de s'inviter dans un débat social, par ailleurs légitime, sur les origines et les conditions de gestion de cette crise[18].

La Chaire UNESCO en prévention de la radicalisation et de l'extrémisme violents a documenté depuis 2021 cette toile de cheffes et chefs de file québécois. À ce moment, ces personnes étaient actives sur plusieurs médias sociaux de masse comme comme Twitter (X), Facebook, Tiktok et YouTube, mais aussi sur des plateformes alternatives permettant de diffuser un discours plus ciblé, comme Telegram, Gab, etc. Les informations diffusées étaient principalement sous-tendues par des idéologies d'extrême-droite, puis d'alterscience et anti-gouvernement. Ces personnes se sont progressivement organisées autour d'une stratégie en réseau, et certaines ont acquis une notoriété leur permettant de développer une activité économique lucrative à partir de leur discours[18, 20]. Depuis la fin de la pandémie, on a vu les discours de cet écosystème s'orienter vers d'autres enjeux de santé publique, mais s'impliquer aussi activement sur les dossiers de l'immigration, de la diversité des identités de genre, ainsi que sur la question des changements climatiques.

Les désordres de l'information : un portrait du phénomène

Si certains désordres de l'informations sont alimentés par un réseau de cheffes et chefs de file, d'autres peuvent se manifester de façon plus constante et insidieuse, en particulier autour de sujets polarisants, faisant appel aux émotions et aux valeurs personnelles. Par exemple, la perméabilité de jeunes face aux discours des influenceurs américains sur les questions de genre (ex. : masculinistes, mouvement anti-LGBTQ+) semble se refléter concrètement dans une baisse du niveau d'aisance des élèves face à la diversité sexuelle et de genre dans les écoles secondaires au Québec[22]. Leur usage de certaines plateformes comme principal outil d'accès à l'information les rendrait plus vulnérables à des discours masculinistes par l'entremise de contenus déclinés sur un spectre allant de l'humour subtil, à la violence explicite[23].

Les périodes électorales au Québec et au Canada sont également propices au renforcement des polarisations et à la circulation d'informations erronées dans les médias sociaux, sur plusieurs aspects. D'abord, par le truchement des opérations d'influence d'États antidémocratiques[16]. Ensuite, par les cheffes et chefs de file diffusant du contenu trompeur ou conspirationniste qui s'activent davantage pendant ces périodes pour tenter d'influencer l'électorat[27]. Enfin, par le jeu des interconnexions sur les médias sociaux, la société québécoise devient plus sensible aux pratiques électorales américaines et européennes, qui ont laissé plus de place aux propos extrémistes et aux pratiques antidémocratiques. Les lignes de fracture politiques émergeant dans ces États culturellement proches du Québec laissent leur empreinte dans notre société.

Quand les désordres de l'information sont alimentés par des scientifiques

Bien que la communauté scientifique ait joué un rôle clé pour communiquer des informations de qualité pendant la pandémie de COVID-19, certaines et certains de ses membres sont tombés dans des pièges les amenant à transmettre des informations qui se sont avérées trompeuses. Par exemple :

- **sortir de son domaine d'expertise;**
- **ne sélectionner que les études en faveur de leurs hypothèses de départ (ex. : Patrick Provost)[26];**
- **ne se baser que sur des études préliminaires (ex : le prix Nobel Luc Montagnier)[24];**
- **ne pas respecter les normes éthiques de recherche visant à protéger les patientes et patients (ex. : études controversées de Didier Raoult)[25].**

Quelques astuces pour évaluer la valeur d'une information scientifique : Fiche 8.

Les désordres de l'information : un portrait du phénomène

Un contexte québécois spécifique

Le Québec se distingue de ses voisins géographiques d'un point de vue social, historique et culturel, et cela se manifeste également dans la manière dont les désordres de l'information s'y déploient. Par exemple, la prédominance de l'usage de la langue française au Québec peut freiner l'accès direct à des discours d'influence américains, mais peut rendre les Québécoises et les Québécois plus perméables à d'autres discours polarisants, issus de France. Coup d'œil sur quelques-unes de ces spécificités qui se révèlent parfois comme des forces, et parfois comme des faiblesses face aux désordres de l'information.

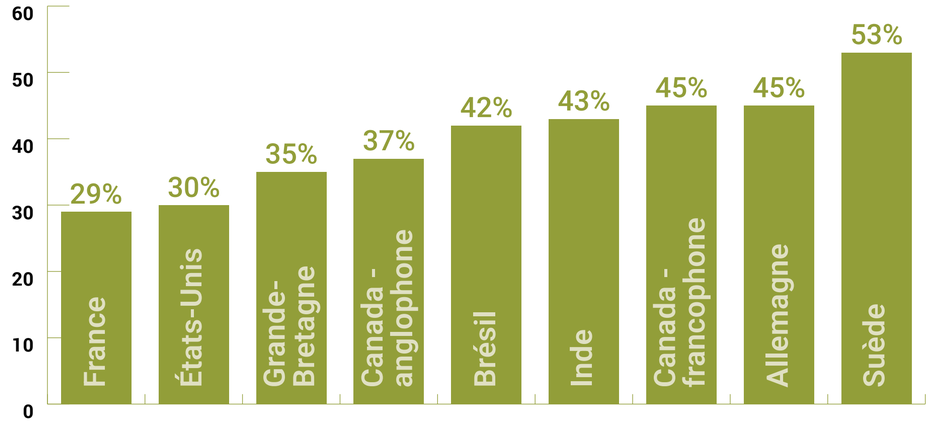
Les habitudes de consommation de l'information

L'accès à des médias non partisans et de qualité pourrait agir comme facteur de protection pour les Québécoises et les Québécois. Dans le même ordre d'idées, les titulaires de charge publique devraient accéder quotidiennement aux ressources médiatiques de qualité[28].

La consommation d'informations sur les médias sociaux augmente le risque d'exposition aux informations erronées[29, 30, 31]. Or, sur ce point la population canadienne francophone (dont la population québécoise francophone) semble se distinguer. Elle manifeste une plus grande confiance dans les médias que la population américaine ou canadienne anglophone. Elle privilégie encore la télévision (45 %) et les sites de nouvelles (28 %) pour accéder aux informations, et a moins recours aux médias sociaux (16 %)[32,33].

La préoccupation de distinguer le vrai du faux tracasse 64 % des Canadiens et Canadiennes, mais seulement 51 % des francophones. Pour vérifier la véracité d'une nouvelle en ligne, 39 % des Canadiens et Canadiennes francophones se tournent vers une source officielle (comme un site web gouvernemental), une proportion similaire aux anglophones. Les influenceurs et influenceuses (54 %) sont les groupes de personnes désignées comme les plus menaçantes en matière de diffusion d'informations fausses ou trompeuses, puis les groupes militants (43 %) et les gouvernements et personnalités politiques de l'étranger (37 %). La population francophone canadienne se distingue des anglophones en identifiant beaucoup moins les personnalités politiques de leur pays comme des menaces sur les médias sociaux (26 % contre 48 % chez les anglophones)[32,33].

Indice de confiance dans les médias, Newman 2025[32]



Les désordres de l'information : un portrait du phénomène

L'adhésion à la pensée conspirationniste au Québec

Le taux de personnes adhérant de manière convaincue ou modérée aux pensées conspirationnistes demeure légèrement plus bas au Québec que dans le reste du Canada. En 2021, elles étaient 6 % d'adhérentes et adhérents convaincus (contre 9 % au Canada) et 15 % d'adhérentes et adhérents modérés (contre 20 % au Canada)[18]. Cette frange minoritaire de la population adhère préférentiellement aux dimensions suivantes (de la plus populaire à la moins populaire) :

- Le contrôle et la manipulation de l'information, par les gouvernements, la science ou les médias. À ce sujet, il n'est pas tant exprimé une méfiance envers la science elle-même qu'envers son assujettissement à des intérêts politiques et corporatistes.
- Les malversations gouvernementales : l'État dissimule son implication dans des activités criminelles, permet des actes terroristes, etc.
- La conspiration mondiale : présence d'un groupe international secret à l'origine d'événements de nature globale.
- Les menaces à la santé et à la liberté.

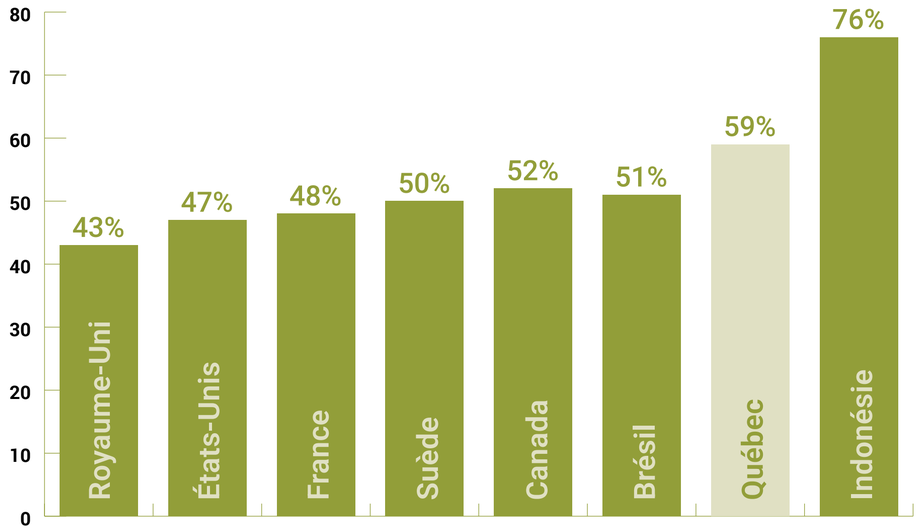
La confiance dans les institutions

Les titulaires de charge publique peuvent agir en veillant à maintenir le lien de confiance avec la population, notamment en adoptant des pratiques de communication qui favorisent l'accessibilité des contenus (voir sous-section Quelques principes de communication publique – p.37).

Il existe un lien significatif entre le manque de confiance dans les institutions et l'adhésion à la pensée conspirationniste[18]. Or, en règle générale, la population québécoise exprime davantage sa confiance que d'autres populations vivant en régime démocratique[34].

Sur d'autres points, la population canadienne suit les tendances générales : elle accorde en premier sa confiance aux scientifiques et au corps professoral, puis aux proches. Les directions d'entreprises et les personnes élues figurent en bas dans le classement[43].

Indice général de confiance dans les institutions (Edelman 2025)[34]



Les désordres de l'information : un portrait du phénomène

Les effets sur les administrations publiques et la démocratie

Les désordres de l'information peuvent, à court comme à moyen terme :

- **Entraver la capacité du gouvernement à protéger le public.** Par exemple, dans le cas d'une crise sanitaire en contribuant au manque d'adhésion aux mesures de santé publique[21], ou dans le cas d'une crise écologique en ralentissant l'adoption de gestes d'atténuation[20].
- **Alimenter la défiance des citoyennes et citoyens envers les institutions.** Ces institutions peuvent notamment être : les gouvernements, l'appareil d'État, la science, et les médias d'information[5, 9].
- **Nuire à la capacité d'établir des consensus sociétaux,** dans un environnement où les points de vue minoritaires clivants sont plus visibles[8].
- **Détourner l'attention de la société québécoise** au détriment d'enjeux nécessitant un engagement soutenu et continu, comme les changements climatiques[20].
- **Affaiblir les capacités du Québec à protéger ses intérêts nationaux,** à cause d'un moindre accès à de l'information neutre et impartiale, et de notre vulnérabilité à l'ingérence étrangère[1].
- **Réduire l'intérêt pour l'engagement politique,** par crainte de s'exposer aux menaces physiques et verbales, en particulier pour les personnes marginalisées ou sous-représentées[9, 16].
- **Mener à des actes de radicalisation et de violence.** Ces actes peuvent revêtir diverses formes : attentats, agressions physiques et verbales, etc.[17]

Le Québec se démarque dans le contexte des désordres de l'information, par ses acquis démocratiques et sociaux. Il bénéficie de médias d'information indépendants, la relation de confiance entre la population et ses institutions se porte bien, et le dialogue social y est possible.

En tant que titulaire de charge publique, vous pouvez agir, à l'échelle individuelle et institutionnelle, afin d'entretenir ces acquis, et ainsi renforcer la résilience québécoise face aux désordres de l'information.

Section 2
Augmentez votre discernement individuel

Fiche 1
Quelques techniques pour tromper les internautes

Vous constatez qu'un groupe de personnes qui étaient jusqu'à présent inconnues dans votre domaine d'activité gagne en popularité sur les médias sociaux. De plus en plus de comptes mentionnent leur nom, les personnes écrivent en anglais, à des heures improbables, par exemple à 4 h le matin. Vous commencez à avoir des doutes sur ces comptes…

En repérant les techniques couramment utilisées pour vous faire parvenir de l'information de façon biaisée, vous serez plus à même de les déjouer et de naviguer à travers le désordre informationnel. En voici quelques-unes.

Hameçonnage

Leurre mis en place par des personnes cybercriminelles pour s'emparer d'informations personnelles. Un courriel avec un lien cliquable reprenant les couleurs d'une institution, par exemple.

Piège à clics

Technique utilisée par certains sites Web qui consiste à utiliser des titres volontairement alarmistes pour attirer l'attention des internautes. Ces sites sont à but lucratif : plus les internautes cliquent, plus les propriétaires de ces sites gagnent de l'argent. Pour faire cliquer les internautes, les rédactrices et rédacteurs ont recours à plusieurs techniques, et font souvent appel aux émotions Fiche 2.

Similitantisme (*astroturfing*)

Les campagnes de similitantisme sont créées par des groupes qui ont pour but d'influencer l'opinion publique pour une cause en utilisant une fausse impression de popularité (création de pages Web, participation aux débats publics, diffusion d'affichage, etc.), voire en simulant un mouvement populaire.

Fermes de robots

Réseau de logiciels automatisés et contrôlés par un seul opérateur pour créer et partager du contenu sur les médias sociaux, et pour interagir avec les internautes, afin de donner de la visibilité à une opinion ou à un sujet particulier, de façon artificielle.

Les robots prennent souvent la forme de profils sans photo ou avec une photo générée par l'intelligence artificielle, au nom étrange (ex. : @quebec75452578). Ils publient des messages formatés de manière identique d'un compte à l'autre, à une fréquence beaucoup plus élevée que les humains, et à des heures qui ne correspondent pas aux « heures normales ».

Pour aller plus loin

Fiche 1
Quelques techniques pour tromper les internautes

Exemples de faux comptes essayant de créer de la visibilité autour d'un sujet :
le modèle de message est identique, l'image et le moment auquel la publication a été effectuée également[35].

Pour aller plus loin

Fiche 2
Méfiez-vous de vos émotions

Qu'est-ce qui vous donne tant envie de cliquer sur ce genre d'articles? Les émotions! Elles jouent un rôle important dans la manière dont on reçoit et on retient l'information, c'est un ressort bien connu dans le monde des communications. Plus une information nous fâche, plus on la partage rapidement… Parfois, la technique est utilisée de manière non éthique dans le seul but de nous faire passer à l'action : cliquer sur un titre, commenter, partager le contenu, etc.[36, 37, 38].

S'il est difficile d'échapper à vos émotions, vous pouvez apprendre à repérer les techniques employées pour les exacerber, afin d'être capables de prendre du recul avant d'agir.

Les informations trompeuses qui font appel à nos émotions contiennent fréquemment :

- **un titre ou un vocabulaire superlatif** (ex. : « la plus grande fraude de tous les temps »);
- **un ton qui s'adresse directement aux internautes** (tu/vous);
- **une mise en opposition entre deux camps** (ex. : « nous, le peuple vs les autres, les élites, le gouvernement »);
- **l'idée d'un secret révélé** (ex. : « voici ce qu'il faut faire pour… »);
- **l'utilisation d'une image triste ou choquante.**

Voici les vrais coupables de l'augmentation de votre facture d'épicerie

Ils jettent des milliers de paquets de bacon aux poubelles pour en faire augmenter le prix. En toute impunité, et dans votre dos.

Fiche 3

Les défauts de votre cerveau : les biais cognitifs

Si vous ne pouvez pas vous débarrasser de votre cerveau, vous pouvez vous entrainer à en repérer les failles.

Pour fonctionner et résoudre des tâches complexes, votre cerveau prend parfois quelques raccourcis[39], comme **les biais cognitifs, qui sont des schémas de pensée trompeurs,** des distorsions de l'information que l'on reçoit et que l'on traite.

Codex simplifié des biais cognitifs[40]

NOTRE MÉMOIRE A SES LIMITES

Notre mémoire n'est pas infinie, ce qui amène notre cerveau à faire le tri de manière sélective dans nos souvenirs.

Effet de primauté
L'information reçue en premier détermine plus l'impression que l'on a d'autrui que l'information reçue ensuite.

Biais de stéréotypes
Nous avons des croyances à la fois positives et négatives au sujet de caractéristiques de divers groupes sociaux.

Effet de négativité
Nous mémorisons davantage des arguments négatifs que des arguments positifs.

Effet de position en série
Nous avons tendance à mieux nous rappeler du premier et du dernier élément d'une série.

TROP PLEIN D'INFORMATIONS !

Notre capacité d'attention est limitée. Ainsi, nous avons tendance à remarquer davantage certaines choses plutôt que d'autres.

Biais de confirmation
Impression que des informations sont jugées plus véridiques lorsqu'elles nous ont déjà été présentées antérieurement dans le passé.

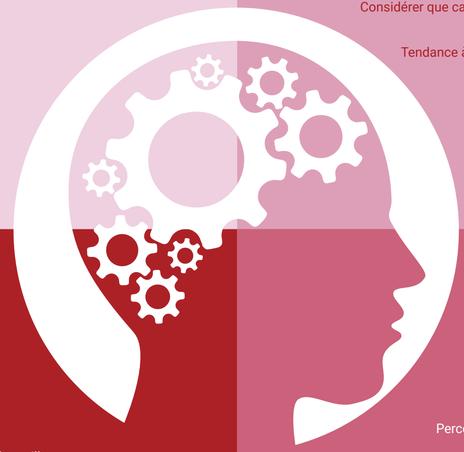
Biais attentionnel
Lorsque nous prenons une décision ou considérons quelque-chose, notre attention est focalisée sur certains facteurs en particulier.

Biais d'omission
Considérer que causer un tort par une action est pire que de causer un tort par l'inaction.

Biais de congruence
Tendance à vouloir mettre en œuvre et tester exclusivement une seule hypothèse, sans tester d'hypothèses alternatives.

Biais de soutien de choix
Tendance à attribuer rétroactivement des attributs positifs à une option que l'on a choisie.

Biais du point aveugle
Tendance à distinguer les biais cognitifs davantage chez les autres qu'en nous-mêmes.



ON DOIT AGIR VITE

Pour ne pas perdre de temps, notre cerveau incite à choisir des options qui paraissent plus simples, ou qu'on a déjà explorées.

Biais du statu quo
Résistance exagérée au changement et préférence pour rester dans notre état initial plutôt que de s'en écarter.

Principe du rasoir d'Okham
Principe selon lequel l'explication la plus simple serait généralement la meilleure et la plus probable.

Biais de croyance
Nous formulons nos hypothèses et nous prenons des décisions en fonction de ce que l'on désire et que l'on se plaît à imaginer, au lieu de prendre en compte la rationalité et la réalité.

Effet d'ambiguïté
Tendance à éviter les options pour lesquelles nous ne disposons pas assez d'information.

Biais d'autocomplaisance
Tendance à attribuer la causalité de notre réussite à nos qualités propres et leurs nos échecs à des facteurs ne dépendant pas de nous.

NOUS AVONS BESOIN DE DONNER DU SENS

Nous imaginons les éléments manquants pour que notre environnement fasse plus de sens pour nous.

Corrélation illusoire
Perception d'une corrélation entre deux événements, corrélation qui n'existe pas ou qui est bien plus faible en réalité.

Effet de compensation morale
La réalisation d'un acte individuel moralement valorisable peut donner lieu à la légitimation d'un acte moralement moins valorisable par la suite.

Effet de notoriété, de halo
Une caractéristique jugée positive à propos d'une personne à rendre plus positives les autres caractéristiques de cette personne.

Biais d'homogénéité de l'exogroupe
Réduction au minimum des différences entre les individus à l'intérieur d'un même groupe qui n'est pas le nôtre.

Biais de projection sociale
Projection sur autrui de nos propres croyances, opinions et visions de la réalité.

Pour aller plus loin

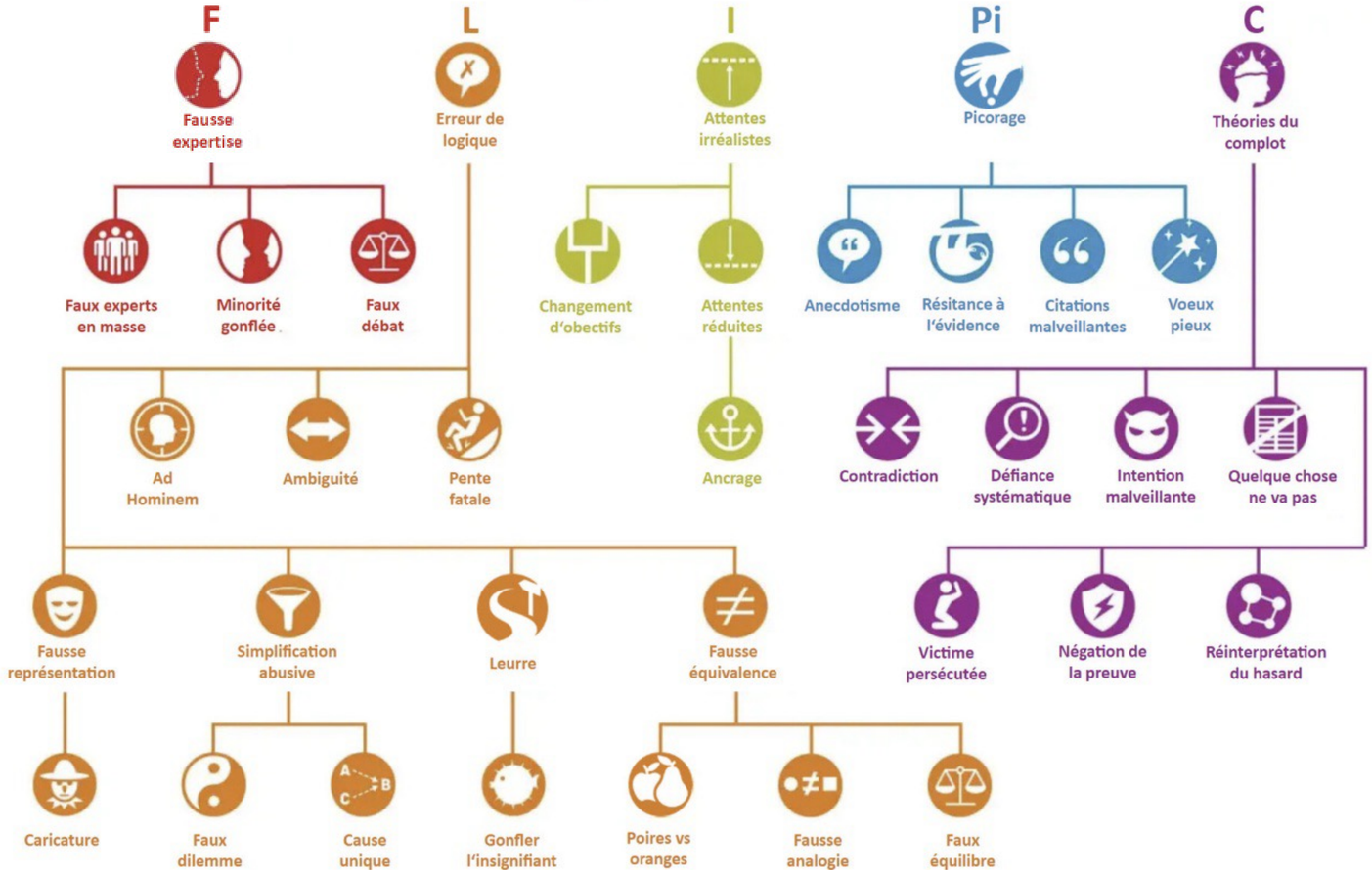
Fiche 4

Les défauts de votre cerveau : les sophismes

Lorsqu'ils sont utilisés de manière consciente, les sophismes s'apparentent à une technique de manipulation, mais bien souvent, les gens en font sans même s'en rendre compte.

Pour fonctionner et résoudre des tâches complexes, votre cerveau prend parfois quelques raccourcis[39]. Dans vos interactions avec les autres, et en particulier quand vous tenez à prouver un point, **vous pouvez céder à la tentation d'opter pour des raisonnements approximatifs :** ce sont les sophismes.

Les techniques du déni de la science[41]



Pour aller plus loin

Fiche 4
Les défauts de votre cerveau : les sophismes

Quelques sophismes courants

Faux expert ou fausse experte

Utiliser le statut d'expert ou d'experte comme sceau de vérité.

Minori|é gonflée

Utiliser le fait que peu de gens partagent une idée pour conclure qu'elle doit être révolutionnaire, ou vraie.

Pente fatale

Suggérer qu'une action mineure entraînera inévitablement des conséquences majeures.

Leurre

Détourner délibérément l'attention vers un point sans importance afin de détourner l'attention d'un point plus important.

Fausse équivalence

Affirmer à tort que deux choses sont équivalentes, alors qu'il existe des différences entre elles.

Faux dilemme

Présenter deux options comme étant les seules possibilités, alors qu'il en existe d'autres.

Attentes irréalistes

Exiger des normes de certitude irréalistes avant de prendre en compte des données scientifiques.

Picorage (*Cherry Picking*)

Citer seulement les faits qui appuient notre argument et ignorer les autres.

Anecdotisme

Utiliser des expériences personnelles ou des exemples isolés en lieu et place d'arguments solides ou de preuves convaincantes.

Théorie du complot

Penser qu'il existe une cause unique à tous les enjeux (par exemple, un groupe de personnes contrôle le monde).

Pour aller plus loin

Fiche 5

Cette nouvelle sur le Web est-elle fiable?

Jouons au jeu des sept erreurs! Au premier coup d'œil, qu'est-ce qui cloche dans cette nouvelle?

http://tribune2QuebecSti

1

LA TRIBUNE DE QUÉBEC

Le Château Frontenac disparaît dans les flammes

Il suffit d'une cigarette mal éteinte par un touriste étranger pour réduire en cendre ce joyau du patrimoine québécois.

5

La rédaction

Un incendie dévastateur ravage l'emblématique hôtel historique

5 février 2025

Québec est en état de choc ce matin suite à un incendie catastrophique qui a complètement détruit le légendaire Château Frontenac, joyau architectural de la ville et symbole mondial de l'histoire québécoise.

L'incendie, dont l'origine reste encore inexpliquée, a commencé aux alentours de 3h du matin. Les pompiers de Québec sont rapidement intervenus, mais la rapidité de la propagation des flammes a rendu leurs efforts pratiquement vains.

Le bâtiment historique, construit en 1893 par la Compagnie de chemin de fer du Canadien Pacifique, a été entièrement consumé en moins de quatre heures. Les autorités sont actuellement en train d'évaluer l'ampleur des dégâts et les possibilités de reconstruction.

Des milliers de citoyens et de touristes ont assisté, impuissants, à la destruction de ce monument qui était bien plus qu'un simple hôtel - il représentait l'âme même de la ville de Québec.

2

RETROUVEZ LA FORME EN 21 JOUR 250-800 $ EN ARGENT COMPTANT !

3

PLAN DU SITE CONCOURS © COPYRIGHT 2025

4

Pour aller plus loin

Fiche 5
Cette nouvelle sur le Web est-elle fiable?

Dans votre quotidien, il est important d'adopter quelques bons réflexes face aux informations que vous consommez, un peu comme quand vous lisez les étiquettes des aliments.

Quelques éléments à vérifier sur les sites Web

(1) URL. La présence d'un cadenas ou de la mention https avant l'adresse permet de savoir si le site est protégé. Pour les sites gouvernementaux québécois et canadiens, seules les terminaisons gouv.ca ou gouv.qc.ca sont utilisées, alors qu'au niveau municipal, les pratiques sont variables.

(2) Hyperlien et publicités. Un site Web contenant beaucoup d'hyperliens et de publicité mérite une attention particulière. Le *backlinking* (ajout de liens entrants) et la publicité sur le Web rapportent des revenus sur la base du nombre de clics et le contenu peut donc voir été créé dans le seul but d'en obtenir.

(3) Point de contact. Les sites Web légitimes offrent toujours plusieurs points de contact (courriel, téléphone, adresse physique). Si cette information est absente, cela devrait vous amener à vous questionner.

(4) Âge du domaine. De façon générale, plus le domaine a été créé il y a longtemps, meilleure est la légitimité du site. Les faux sites de nouvelles sont souvent créés rapidement et ont une durée de vie plus courte.

(5) Source. Certaines sources d'information sont considérées comme plus crédibles : les sites institutionnels et les sites des médias d'information. Les contenus publiés sur des blogues personnels et les médias sociaux demandent un examen plus attentif. En cas de doute, croisez vos sources!

Témoin de navigation. Les sites Web canadiens sont tenus par la loi d'utiliser une fenêtre contextuelle pour mentionner leur usage de témoins (*cookies*). Si un site Web n'en a pas, ce n'est peut-être pas une entreprise canadienne qui en est propriétaire. N'oubliez pas que vous avez la liberté d'accepter ou non l'utilisation de ces témoins! Fiche 9

Contenu. Parfois, le contenant donne l'apparence d'un site Web légitime, mais le contenu ne l'est pas : il est truffé de fautes ou d'informations erronées, ne semble pas avoir été relu avant publication. Lorsque des faits ou des données sont rapportés, est-ce qu'on fait mention de la source d'information?

Pour aller plus loin

Fiche 6
Confirmez la véracité d'une image ou d'une vidéo

Les outils basés sur l'IA sont capables de générer des images et des sons très réalistes, et ce, presque instantanément[12], ce qui rend la distinction entre le vrai et le faux de plus en plus difficile, voire impossible à l'œil nu. Si vous avez un doute sur une image ou une vidéo, voici des astuces et des outils qui peuvent vous aider à y voir plus clair.

Portez attention au contexte

De façon générale, si une image semble trop invraisemblable pour être vraie, c'est qu'elle ne l'est probablement pas! En portant attention au contexte d'utilisation et aux propos associés, vous aurez déjà un bon indice de la fiabilité de cette image.

Saurez-vous voir ce qui cloche dans cette image générée par l'IA?

Pour aller plus loin

Fiche 6
Confirmez la véracité d'une image ou d'une vidéo

Effectuez une recherche inversée

Parfois, une image prise lors d'une inondation ou d'une guerre est reprise pour illustrer d'autres événements similaires… Et cela porte à confusion. Pour éviter de tomber dans ce piège, vous pouvez utiliser la recherche inversée afin de savoir où et quand l'image a été prise, ou si elle a été créée de toutes pièces. Elle permet également de croiser les sources, c'est à dire de vérifier si l'image se trouve aussi sur des sites crédibles et reconnus.

- Sur votre téléphone intelligent : utilisez les applications gratuites **Google Lens**, **Reverse Photo App** ou **Tiny Eye** pour authentifier des images, où que vous soyez.
- Sur votre ordinateur, la méthode la plus simple consiste à effectuer une recherche inversée sur **Google Image/ Lens** : téléchargez l'image et glissez-la dans la barre de recherche.

Repérez les défauts dans l'image

Certaines failles demeurent dans les logiciels de génération d'images par l'IA et peuvent éveiller votre vigilance :

- manque de cohérence ou de précision (nombre de doigts sur une main ou longueur des membres);
- manque de netteté dans les représentations de grands groupes/foules;
- texture de la peau qui semble très lisse;
- difficulté à intégrer le texte dans une image (nom de marque sur un produit, affiche au mur, etc.)[43];
- dans les vidéos, les visages ou les cheveux ne bougent pas naturellement.

La technologie évolue rapidement!

Les failles que l'on retrouve actuellement dans les images seront probablement corrigées à long terme, rendant la détection des fausses images plus ardue[12, 43].

Pour aller plus loin

Fiche 7

Réduisez votre dépendance aux algorithmes

Vous aimez bien le ski de fond, mais… Pourquoi votre fil de nouvelles sur les médias sociaux en est soudainement envahi, depuis deux semaines ?

Sur les médias sociaux, les algorithmes sont des programmes informatiques qui sélectionnent des contenus pour vous, selon vos intérêts : si vous aimez une publication sur la victoire des Canadiens de Montréal, vous verrez du contenu en lien avec le hockey. Cette exposition à du contenu qui rejoint vos intérêts peut rapidement vous faire glisser dans une bulle de filtre, une chambre d'écho[44, 45] où tout ce que vous voyez tourne autour d'un même sujet ou d'une même vision du monde. Ceci peut renforcer certains de vos biais Fiche 3 et vous rendre vulnérable aux personnes qui cherchent à attirer votre attention plutôt qu'à vous informer.

Vous pouvez poser les gestes suivants afin de réduire votre dépendance à ces algorithmes, et ainsi avoir un meilleur contrôle sur les informations que vous consommez.

- **Faites le ménage :** désabonnez-vous des pages dont le contenu n'est plus d'intérêt pour vous.
- **Abonnez-vous aussi à des comptes d'institutions de référence** et dont la crédibilité est reconnue (gouvernements, organisations internationales, médias fiables et indépendants).
- **Ouvrez vos horizons :** et si vous suiviez aussi des pages qui diffusent des points de vue opposés à vos opinions? Cela permettrait de briser vos éventuelles chambres d'écho.
- **Diversifiez vos sources d'information :** informez-vous aussi en dehors des médias sociaux, par l'entremise d'applications et sites de médias d'information, par exemple.
- **Paramétrez vos médias sociaux :** désactivez les liens entre votre compte et vos recherches à l'extérieur de la plateforme, créez des « listes » dans lesquelles vous n'entrez que les comptes que vous voulez suivre.
- **Effacez de temps en temps votre historique de recherche** sur les plateformes numériques (la procédure à suivre varie d'une plateforme à l'autre).
- **Et si vous optiez pour un fil RSS?** Il permettra de regrouper sur une seule page tout le contenu que vous souhaitez suivre.

Fiche 8
Évaluez la valeur d'une information scientifique

Dans un débat à la télévision, vous entendez la phrase « Ce n'est pas moi qui le dis, c'est la science ». Certes, mais de quelle science s'agit-il? Dans quelle mesure cet argument met-il fin aux discussions?

L'information scientifique est considérée comme une information particulièrement fiable, au regard des chroniques d'opinion, ou des témoignages par exemple, du fait qu'elle se base sur l'application d'une méthode rigoureuse et systématique : la méthode scientifique. Cependant, qu'entend-on par « information scientifique », et comment en évaluer la valeur? Voici quelques balises pour vous y retrouver, même sans doctorat!

Comment fonctionne la science?

La science est un processus incrémental, dans lequel chaque résultat scientifique est évalué et validé par un comité de pairs[36,46]. Ainsi, les études scientifiques peuvent éventuellement être réfutées par d'autres, plus solides, plus actuelles, plus pertinentes. De ce fait, plutôt que de vous baser sur une seule étude, **vous devriez vous fier à un certain niveau de consensus scientifique[41],** soit quand un certain nombre d'études sur un sujet pointe dans une même direction.

À prendre en considération durant la lecture d'une information scientifique

En plus des éléments propres aux nouvelles en ligne évoquées dans la Fiche 5, vous devriez porter attention aux points suivants :

- Si le titre promet des avancées scientifiques extraordinaires, méfiez-vous (ex. : un nouveau traitement qui guérit le cancer)!
- Les autrices, auteurs ou les spécialistes cités s'expriment-ils ou elles dans leur domaine d'expertise?
- Les sources citées devraient principalement être des publications dans des revues ou des conférences scientifiques.
- Les propos devraient s'inscrire dans un consensus scientifique.

Vous souhaitez pousser votre vérification un peu plus loin?

Vous gagnerez peut-être à faire appel à des renforts, soit si vous n'avez pas l'habitude de naviguer dans les publications scientifiques, soit parce que le sujet traité est hors de votre domaine d'expertise. N'hésitez pas à interpeler des membres de la communauté de recherche, le cas échéant.

Pour aller plus loin

Fiche 8
Évaluez la valeur d'une information scientifique

Quelques pièges courants reliés aux nouvelles scientifiques…

dans lesquels peuvent tomber les journalistes comme leur public!

- **On extrapole à l'être humain des résultats obtenus *in vitro* ou sur des animaux.** Ce n'est pas parce qu'une étude a été réalisée sur des souris ou dans des éprouvettes que ses conclusions s'appliquent à nous.
- **On confond la corrélation avec la causalité.** Plusieurs études établissent des liens entre l'incidence de maladies et des habitudes alimentaires, mais pas nécessairement des liens de cause à effet. Ex. : ce n'est pas parce que le coq chante tous les matins au moment où le soleil se lève qu'il est à l'origine du lever du soleil.
- **On parle de proportions relatives versus de proportions absolues.** Ex. : si les personnes mangent 50 g supplémentaires de viande transformée tous les jours, leur risque de cancer du côlon augmente de 18 %. Ça vous parait énorme? Ramené à des proportions absolues, cela représente environ un cancer de plus par 1000 personnes, sur une période de 10 ans. Un chiffre bien moins effrayant[47]!
- **Les études sont citées hors de leur contexte.** Ex. : ce n'est pas parce qu'un phénomène social a été observé en Autriche qu'il se manifeste de la même manière au Québec.

Pour aller plus loin

Fiche 9

Comment se porte votre empreinte numérique?

Avez-vous posé l'un ou l'autre de ces gestes, ces derniers mois?

- **consulter le fil d'actualités d'un média social;**
- **utiliser la carte de fidélité de votre épicerie préférée;**
- **utiliser le GPS de votre téléphone pour vous rendre à une rencontre professionnelle;**
- **répondre à l'appel téléphonique d'une personne inconnue.**

Si oui, ceux-ci sont tous susceptibles d'avoir renforcé votre empreinte numérique!

Pour aller plus loin

Dès que vous utilisez une technologie numérique, vous êtes susceptible de laisser une petite trace de votre passage, parfois même sans le savoir… un peu comme on laisserait des empreintes digitales sur les objets qu'on utilise. Toutes ces informations mises ensemble constituent votre empreinte numérique, et peuvent être utilisées par d'autres pour anticiper vos comportements ou ceux de votre organisation, via les outils d'intelligence artificielle[16].

Est-ce grave de laisser une empreinte numérique derrière soi?

Il est tout à fait normal d'avoir une empreinte numérique, cependant celle-ci peut :

- créer une faille de cybersécurité pour votre organisation, en particulier lorsqu'elle s'additionne avec celle de collègues ou de partenaires;
- augmenter votre risque d'être victime d'usurpation d'identité, sur les médias sociaux, auprès des administrations publiques, des institutions bancaires, etc.;
- vous exposer à des campagnes ciblées d'influence, affecter à moyen terme votre crédibilité, et indirectement l'autonomie du Québec au regard d'autres nations et de divers intérêts Fiche 11.

Partager ses performances de course à pied sur Strava

Une enquête publiée dans le journal *Le Monde* en 2024 a démontré comment l'utilisation de l'application sportive Strava a permis d'anticiper les futurs déplacements et lieux de séjour de plusieurs présidents, comme Emmanuel Macron, Joe Biden et Vladimir Poutine[48, 50].

Fiche 9

Comment se porte votre empreinte numérique?

Comment limiter votre empreinte numérique[49]?

- **Prenez le temps qu'il faut,** face à la multitude d'actions que vous posez dans l'univers numérique (création de comptes, remplissage de formulaires, etc.).
- **Adoptez des réflexes de sobriété numérique.** Lorsque vous utilisez des logiciels en ligne, demandez-vous s'ils offrent une réelle plus-value, en particulier pour les logiciels utilisant de l'IA générative Fiche 15.
- **Remplissez les champs obligatoires des formulaires,** et interrogez-vous sur la pertinence de fournir les informations optionnelles.
- **Désactivez les témoins,** autant que possible, lorsque vous entrez dans un espace numérique. Ces témoins gardent en mémoire votre activité sur le site Web (historique de navigation, de connexion ou d'achat). Normalement, ces informations sont utilisées pour vous offrir une expérience personnalisée, mais elles peuvent aussi être partagées et utilisées à votre insu pour d'autres fins.
- **Prenez connaissance des politiques de confidentialité et des conditions d'utilisation** des outils numériques, notamment le type d'information recueillie et leurs conditions de gestion. En cas de doute, consultez les responsables de la protection des renseignements personnels, les responsables des habilitations de sécurité ou les responsables de la sécurité des systèmes informatiques de votre organisation.
- **Faites un tour de vérification des paramètres de vos applications** pour limiter les accès publics et les paramètres qui impliquent l'accès à votre emplacement, votre calendrier, vos contacts, etc.

Pour aller plus loin

Section 3
Augmentez votre discernement institutionnel

Quelques principes de communication publique

Dans le grand marché de l'attention régi par les algorithmes, **les administrations publiques doivent inspirer confiance[28, 51], tout en permettant aux citoyens et aux citoyennes d'exercer leur esprit critique afin de vérifier le bien-fondé de chaque décision[52]**. Voici quelques principes de communication publique qui permettent d'atteindre cet équilibre.

Transparence[7, 28, 53]

Bien que la communication des organismes publics soit encadrée par la législation, les règlements de sécurité publique et le devoir de réserve, vous devriez être en mesure d'assumer un certain risque corporatif au profit d'une communication plus transparente avec la population. Communiquez les informations de manière honnête et exhaustive, y compris les sources qui les sous-tendent, les processus de décision, les incertitudes et les changements de cap.

Pertinence[53]

Réfléchissez à la plus-value de l'information que vous diffusez, afin de vous assurer qu'elle réponde à un besoin avéré. Ainsi, vous ne contribuerez pas à alimenter à votre insu le bassin des informations non pertinentes circulant sur les médias sociaux.

Clarté

Évitez l'utilisation de termes propres aux politiques publiques ou de termes techniques. Vous pouvez vérifier et ajuster la clarté de vos communications, de plusieurs manières : relecture par les publics cibles, enquête sur les irritants liés à l'utilisation des services, utilisation de personas, etc.

Pour aller plus loin

Quelques principes de communication publique

Accessibilité[53]

Redoublez d'efforts pour rejoindre les personnes les plus vulnérables, les plus désengagées ou avec des handicaps, en diversifiant les canaux de communication. Adoptez des pratiques de conception de pages web qui permettent aux utilisateurs et utilisatrices de trouver l'information plus facilement sur les plateformes numériques.

Constance et cohérence[53]

Utilisez les mêmes canaux officiels, les mêmes visuels, des termes cohérents et le même message dans l'institution, et si possible, d'une institution à l'autre.

Crédibilité[46]

Les messages doivent être portés par des personnes ou des organismes inspirant confiance. Soutenez vos propos par des faits, par des études scientifiques ou par l'autorité de personnes expertes, et rendez ces sources disponibles. Au besoin, faites appel à des porte-paroles en relation avec vos publics cibles.

Prévention[28]

Repérez au plus tôt les enjeux nécessitant de la communication Fiche 10 et agissez en amont afin de réduire les risques de rumeurs ou de spéculation Fiche 14.

Adaptabilité

Adaptez vos communications aux changements rapides de l'environnement et aux besoins que les personnes expriment. Cela peut impliquer de donner plus de précisions, d'utiliser un vocabulaire différent, d'aborder des sujets connexes, etc.

Pour aller plus loin

Sous-section 3.1
Actions proactives

Tout ce que vous pouvez faire pour prévenir les effets des désordres de l'information sur votre institution.

Fiche 10
Veille ciblée : déployez vos antennes

Votre organisation vient de lancer une campagne pour promouvoir l'outil d'optimisation de la consommation d'énergie pour les bâtiments. La réception est bonne, les téléchargements de l'outil augmentent. Mais en parallèle, le mouvement « anti-ondes électromagnétiques » reprend de l'ampleur… Vous vous rendez compte que certains porte-paroles de ce mouvement ont repris votre campagne à leur compte.

En intégrant une veille ciblée à toutes les étapes de vos projets, en particulier sur les sujets que vous savez sensibles, vous pourrez détecter non seulement l'émergence de mouvements ou d'opérations d'influence, mais aussi les inquiétudes sociétales sous-jacentes qui les alimentent. La compréhension fine de ces dynamiques sociales devient alors un atout stratégique en temps de crise Fiche 17.

Quelques outils de veille

- **Organisez votre veille institutionnelle.** Le Réseau stratégique de veille et de prospective (RSVP) du gouvernement du Québec propose quelques outils simples d'approche, ainsi qu'une communauté de pratique.
- **Utilisez les options analytiques des plateformes de médias sociaux,** pour savoir en temps réel comment vos messages circulent.
- **Utilisez des agrégateurs de contenu** (Hootsuite, Sprout, Agorapulse, Google Trends, etc.) pour suivre chaque mention de votre nom.
- **Explorez la veille augmentée par l'IA!** Des outils comme Polly offrent l'analyse de sentiments, et la prédiction de comportements, ou détectent les discours haineux (ex. : SAMbot)[54].

De fréquentes tactiques d'évitement

Certaines personnes ont intérêt à ne pas se faire repérer! Voici les techniques qu'elles utilisent régulièrement :

- **Substituer des mots-clés surveillés par des variantes orthographiques, utiliser des métaphores ou des euphémismes, utiliser des émojis pour remplacer des lettres.**
- **Fragmenter les messages en plusieurs publications.**
- **Utiliser des images contenant du texte pour éviter la détection textuelle.**
- **Alterner entre plusieurs comptes coordonnés tout en restant sous les seuils d'activité suspects.**
- **Créer des « conversations miroirs » sur des plateformes secondaires, et utiliser les médias sociaux populaires uniquement pour des redirections.**

Pour aller plus loin

Fiche 10
Veille ciblée : déployez vos antennes

Pour une veille responsable

- **Adaptez constamment vos critères de recherche :** ils doivent être justifiables au regard de votre mission, et vous devrez les adapter régulièrement pour répondre aux tactiques d'évitement utilisées par certains internautes.
- **N'intégrez jamais d'informations personnelles, confidentielles ou sensibles dans les requêtes**[55]**.**
- Pour limiter les risques, vous pouvez activer certaines options sur les navigateurs Internet.
- Dans quelle mesure les informations que vous manipulez sont-elles sensibles?
- **La loi ne vous autorise pas à effectuer de veille dans des sphères privées.** Si certains comptes affichent clairement leur statut public ou privé, d'autres se situent dans une zone grise (groupes privés, mais largement ouverts, etc.). En cas de doute ou d'ambiguïté, consultez le service juridique de votre organisation.
- **Lorsque vous ciblez des groupes, pensez aux biais qui vous entourent.** Dans quelle mesure ce ciblage est-il justifié? Prenez en compte vos propres biais cognitifs Fiche 3 et ceux inhérents aux algorithmes de certains outils numériques.
- **Vous utilisez les services de compagnies** pour effectuer de la veille ciblée? Tentez de vérifier dans quelle mesure ces dernières répondent aux bonnes pratiques évoquées plus haut.

Pour aller plus loin

Fiche 11
Évaluez les risques d'opérations d'influence

Plusieurs États comme la Russie, la Chine[16], utilisent la désinformation comme une cyberarme pour déstabiliser les démocraties. En tant que titulaire de charge publique, vous pourriez être vulnérable à ces opérations d'influence. Il est important que vous soyez en mesure de les repérer, afin de protéger votre institution. Ces dernières sont parfois difficiles à détecter, car elles peuvent prendre la forme de manœuvres diffuses de parties prenantes non gouvernementales, mais certains indices devraient vous mettre la puce à l'oreille…

Points de vigilance au Québec et au Canada

Les activités d'influence étatique. Selon un rapport du Centre canadien pour la cybersécurité évaluant les principales cybermenaces pour 2025-2026, il faut faire preuve de vigilance vis-à-vis des activités de la Chine et de la Russie principalement, ainsi que l'Iran, la Corée du Nord et l'Inde[56]. Ces menaces changent rapidement, notamment à cause de l'évolution des politiques américaines, non encore documentées dans ce rapport.

Les domaines d'activité sensibles. Portez une attention particulière aux investissements étrangers et aux collaborations de recherche et développement pour :

- **L'exploitation de minéraux critiques et stratégiques**[57], comme le graphite, le nickel, le cobalt et les éléments du groupe du platine, le lithium, les terres rares, le titane, le niobium, le zinc et le cuivre;
- **Les technologies considérées comme sensibles**[58] **:** infrastructures numériques, intelligence artificielle et mégadonnées, robotique et systèmes autonomes, technologies aérospatiales, etc. (voir la liste complète dans la section Pour aller plus loin).

Quelques techniques d'ingérence[62]

- élicitation : soutirer des informations;
- relations sociales intéressées;
- coercition : chantage et menaces;
- corruption et financement illégal;
- cyberattaques : via le hameçonnage;
- désinformation sur les médias sociaux.

Pour aller plus loin

Fiche 11
Évaluez les risques d'opérations d'influence

Distinguez l'influence légitime de celle qui ne l'est pas

Il est accepté que des personnes mènent des opérations d'influence auprès des décisionnaires politiques, de manière transparente et avec des moyens légitimes (voies diplomatiques, activités encadrées par Lobbyisme Québec)[59]. Cela devient problématique lorsque des personnes ou des organisations :

- **manquent de transparence.** Affiliations masquées, octroi occulte de financement, actions coercitives sur des individus, etc;
- **ont une intention malveillante.** Volonté d'acquérir un avantage géopolitique, militaire ou stratégique au détriment des intérêts du gouvernement en place.

Toutes sortes d'activités se situent dans une zone grise en matière de légitimité, dans laquelle il convient de faire preuve de vigilance[60], et notamment dans le cyberespace, qui est très peu réglementé.

Posez les bons gestes[62]

- **Mettez à jour vos pratiques de cybersécurité,** par exemple sur la base de la Directive gouvernementale[63] et du *Guide de sensibilisation sur la sécurité de l'information* du gouvernement du Québec.
- **Mettez en place une veille ciblée,** en particulier dans des domaines d'activités sensibles cités plus haut Fiche 10.
- **Assurez-vous de bien connaître vos partenaires,** leurs intentions, leur affiliation étatique et idéologique, etc.
- **Informez votre personnel et vos partenaires** de votre posture et de vos politiques en matière d'opérations d'influence.
- **Signalez toute activité suspecte et tout incident** d'intimidation, de harcèlement, de coercition ou de menace aux autorités de votre institution, au Service canadien du renseignement de sécurité, ou à votre service de police local.
- **Poursuivez et diversifiez des activités diplomatiques saines** dans votre domaine d'activité, notamment les activités de diplomatie scientifique qui permettent de renforcer notre capacité collective à accéder aux données probantes à l'échelle mondiale[64].

Pour aller plus loin

Fiche 12
Configurez les médias sociaux

Les médias sociaux constituent de bons canaux de communication avec les publics cibles de vos organisations, en particulier pour rejoindre les plus jeunes, pour qui ils constituent les canaux privilégiés d'accès à l'information. Cependant, ils peuvent aussi rendre les institutions et les personnalités publiques vulnérables. Pour profiter au maximum des bienfaits de ces plateformes tout en prévenant leurs effets négatifs, voici quelques bons réflexes à adopter.

Pour prévenir les risques d'usurpation d'identité et d'opérations d'influence[65]

- **Optez pour les médias sociaux les plus sécuritaires,** qui offrent de bonnes conditions de sécurité de l'information (ex. : utilisation prudente de TikTok). Tenez-vous au courant des conditions d'utilisation des médias sociaux qui peuvent évoluer dans le temps!
- **Sécurisez l'accès à vos applications de médias sociaux.** Utilisez un mot de passe robuste, autorisez l'accès à un nombre limité de personnes, activez l'authentification multifactorielle lorsque c'est possible, consultez les comptes sur un réseau de téléphonie mobile ou un réseau Wifi sécurisé, installez les mises à jour.
- **Utilisez les systèmes d'authentification des comptes officiels corporatifs** ou des personnalités publiques, offerts par les plateformes numériques pour prévenir les fraudes à l'identité.
- **Éditez les paramètres de confidentialité** selon l'usage que vous souhaitez en faire pour votre organisation. Établissez notamment qui peut vous suivre, qui peut voir vos publications.
- **Adoptez des pratiques sécuritaires d'utilisation.** Séparez autant que possible votre vie personnelle et professionnelle sur les plateformes, évitez d'utiliser les comptes institutionnels pour vous connecter à des applications ou à des sites tiers, évitez de partager des informations personnelles Fiche 9.
- **Effectuez une veille sur les médias sociaux,** pour repérer les utilisations frauduleuses de votre institution ou de votre image publique Fiche 10.

Pour aller plus loin

Fiche 12
Configurez les médias sociaux

Pour prévenir le harcèlement et la diffamation

- **Animez les espaces de dialogue** reliés à vos publications, ou désactivez-les Fiche 13.

En cas d'incident…

- **Utilisez les outils de signalement des contenus et de comptes.** Attention, les propos ou comptes signalés doivent contrevenir à une loi (discours haineux, diffamation, etc.) Fiche 20.

Que pouvez-vous dire dans vos médias sociaux personnels?

Avez-vous le droit de donner votre opinion pendant une campagne électorale? Pouvez-vous communiquer de l'information sur des programmes gouvernementaux?

Dès que vous publiez quelque chose sur les médias sociaux, cela est considéré comme de l'information publique[66]. Donc, même si vous faites un usage personnel[67] de vos médias sociaux, vous devriez toujours garder à l'esprit votre devoir de loyauté envers l'employeur[68, 69]. Par exemple, si vous travaillez pour le ministère de la Santé et des Services sociaux, un commentaire négatif de votre part sur la gestion d'une campagne de vaccination peut être condamnable[70].

Par ailleurs, en général les institutions publiques désignent des personnes qui peuvent parler en leur nom, et ce sont celles-ci qui sont habilitées à répondre aux questions des citoyennes et des citoyens en ligne.

Pour aller plus loin

Fiche 13
Animez les espaces de dialogue

Une internaute très active sur Facebook commente systématiquement les publications de votre organisation, en critiquant vos services. Votre équipe de communication passe beaucoup de temps à lui répondre, et vous commencez à vous interroger. Devriez-vous limiter vos échanges avec elle? Lui demander d'arrêter? Et si vous désactiviez les zones de commentaires sous vos publications?

Avec les médias sociaux et les services de consultation en ligne, les occasions d'établir des espaces de dialogue entre les institutions et les publics se multiplient dans le cyberespace. Comment profiter au maximum de ces espaces de dialogue, tout en limitant les risques que cela dérape?

Avez-vous bien ciblé vos besoins?

Vous devriez ouvrir des espaces de dialogue avec une **intention précise** en tête, et y associer **des ressources suffisantes**. Dans le cas contraire, vous créez la perception que les contributions des internautes ne sont pas réellement les bienvenues, et augmentez le sentiment de distance entre votre institution et la population.

Établissez des règles du jeu

Mettez en place une netiquette et/ou un code de conduite, qui précise les modalités d'interaction acceptables et sécuritaires pour toutes et tous, et les limites des sujets abordés. Affichez-les et rappelez-les régulièrement. En cas de situation ambiguë, vous pouvez consulter le service juridique de votre organisation.

Quelle est votre posture dans les discussions?

Si vous êtes responsable dans votre institution publique de gérer un espace de dialogue numérique :

- **Vous devez minimalement offrir des informations factuelles et accessibles** pour poser les bases d'un échange éclairé (voir sous-section Quelques principes de communication publique, p. 36);
- **Vous pouvez aussi prendre part au dialogue avec les internautes,** dans les limites de la politique adoptée par votre institution. Ex. : répondre aux questions sur vos services, expliquer les choix de votre organisation, partager des sources qui ont sous-tendu les décisions.

Vous ne maîtrisez pas :

- l'actualité;
- les comportements humains;
- les algorithmes des plateformes de médias sociaux;
- les opinions des personnes convaincues;
- la réception de vos messages dans les médias sociaux.

Pour aller plus loin

Fiche 13
Animez les espaces de dialogue

Lorsque les échanges revêtent une dimension partisane ou idéologique :

- **Si vous êtes membre d'une administration publique**, en règle générale le devoir de réserve vous incite à ne pas participer à ces discussions au nom de votre organisation.
- **Si vous appartenez à la sphère politique,** il est tout à fait justifié que vous contribuiez à ces débats, qui sont le signe d'une démocratie ouverte à la critique et à la contestation Fiche 16.

Pour éviter que vos interactions en ligne ne dérapent[71]

- Utilisez les faits pour étayer vos réponses.
- Optez pour un langage constructif, afin d'éviter les spirales négatives.
- Évitez les réactions à chaud : vérifiez l'information et prenez votre temps avant de répondre.
- Faites preuve d'empathie, ne présumez pas que les personnes sont mal intentionnées.
- Changez votre perception des échanges en ligne : ils ne prennent pas toujours la forme de joutes oratoires dans lesquelles il y a des personnes gagnantes et d'autres perdantes.
- Limitez vos interactions à un ou deux aller-retours seulement.

Pour aller plus loin

Fiche 14
Mieux vaut prévenir que guérir… l'inoculation

L'inoculation (*prebunking*) est une technique de communication qui consiste à offrir des outils pour « immuniser » les gens contre les informations erronées avant qu'elles ne leur parviennent[72], un peu comme on utiliserait un vaccin pour limiter la propagation de la grippe. Elle a comme premier objectif de bâtir une relation de confiance avec les publics et d'en renforcer la résilience, notamment en prévision de périodes de crise[3, 72].

L'inoculation s'appuie sur plusieurs éléments. Elle peut être :

- **Basée sur les faits.** Corriger une affirmation fausse à l'aide de données probantes, avant que celle-ci ne se propage largement. Cela implique que vous bénéficiez d'une veille performante Fiche 10.
- **Basée sur la logique.** Expliquer les tactiques utilisées pour manipuler l'information et comment s'en protéger[73], à l'image de la première partie de ce guide. C'est cette forme qui présenterait le plus grand bénéfice. À ce titre, de nombreuses ressources en littératie numérique et scientifique sont accessibles gratuitement (voir section Pour aller plus loin)[72].
- **Basée sur les sources.** Pointer les sources d'informations non fiables. Dans le cas des institutions publiques, à utiliser avec parcimonie, pour ne pas renforcer des perceptions du type « État censeur » ou « État prescripteur de la vertu » Fiche 18.

Exemple d'inoculation basée sur la logique

En expliquant à la population que l'industrie du tabac a fait appel à de fausses expertises dans les années 1960 pour alimenter le débat sur les effets néfastes du tabac, celle-ci devient plus consciente que de telles techniques peuvent être utilisées, dans le contexte des changements climatiques, par exemple[74].

Pour aller plus loin

Fiche 14
Mieux vaut prévenir que guérir… l'inoculation

Une campagne d'inoculation efficace

- **Devrait suivre les grands principes de communication publique** (voir sous-section Quelques principes de communication publique, p. 36).
- **Fait écho à des événements récents et aux expériences vécues des individus.** Cela commande donc de permettre aux individus de prendre la parole.
- **Fait appel à la responsabilité collective** en évoquant des valeurs partagées et des sentiments comme l'empathie ou l'agentivité (ex. : vérifions la crédibilité des informations avant de les partager, informons notre entourage, etc.).
- **N'est pas menée dans l'intention de convaincre ou de persuader,** mais simplement d'informer.

Inoculation ou démystification : privilégiez la prévention

Lorsqu'il est possible de choisir, l'inoculation est une approche à privilégier au regard de la démystification Fiche 19[72, 73].

- Sa dimension proactive renforce la perception d'**un État qui assume sa fonction de protection** de la population et qui s'engage pour elle.
- Sa dimension éducative renforce la **résilience face aux crises.**
- Elle permet à l'État de diffuser **moins de messages négatifs,** propres à la démystification[6,].

Pour aller plus loin

Fiche 15
Utilisation responsable de l'intelligence artificielle générative

Les outils d'intelligence artificielle (IA) générative promettent de révolutionner les services publics : utilisation d'agents conversationnels, création de contenus, etc.[75,76]. Cependant, leur adoption mobilise beaucoup de ressources, et s'inscrit dans un jeu de pouvoir international et suscitera de grands bouleversements[11].

Dans ce contexte, tous les titulaires de charge publique partagent la responsabilité collective d'utiliser ces outils de manière responsable et sécuritaire. À chaque fois que vous vous apprêtez à utiliser un outil d'IA générative ou un agent conversationnel, posez-vous ces six questions, qui s'appuient sur l'Énoncé de principes pour une utilisation responsable de l'IA par les organismes publics[76].

Est-ce autorisé?

D'abord, est-ce que l'usage que vous vous apprêtez à faire de l'IA respecte le cadre légal existant? Par exemple :

- Vous ne devriez pas demander aux outils d'IA de copier des productions soumises à des droits d'auteur.
- Vous ne devriez pas chercher à tromper vos publics cibles en vous faisant passer pour une personne connue, sans son consentement.
- N'entrez pas dans des outils d'IA des informations personnelles, confidentielles, sensibles ou qui font l'objet de propriété intellectuelle.

Le coût environnemental de l'IA[77]

Une requête sur une IA générative nécessite 30 fois plus d'énergie qu'une requête sur un moteur de recherche classique.

62 millions de tonnes de déchets électroniques ont été produits en 2022 dans le monde, avec une projection de +32 % d'ici 2030.

Pour aller plus loin

Fiche 15
Utilisation responsable de l'intelligence artificielle générative

Ensuite, informez-vous sur les directives de votre organisation en matière de l'usage de l'IA. Les ministères et organismes publics québécois suivent les directives du ministère de la Cybersécurité et du numérique, et ils peuvent aussi émettre davantage d'instructions, plus précises et contextualisées.

Est-ce réellement utile?

Avez-vous vraiment besoin d'utiliser un logiciel basé sur l'IA et branché sur un jeu de données pharaonique, pour corriger un courriel? Utilisez ces outils de manière proportionnelle à vos besoins, afin de prévenir les expositions inutiles de votre organisation aux vulnérabilités propres aux technologies de l'IA, et les émissions de gaz à effet de serre associées à ces solutions technologiques.

Si vous êtes gestionnaire, vous souhaiterez aussi prévenir la dépendance technologique de vos équipes, notamment pour les tâches analytiques ou décisionnelles.

Est-ce sécuritaire?

Privilégiez les IA entraînées par un corpus de données délimité et interne. Dans le cas contraire, vérifiez les conditions d'utilisation des données que vous entrez dans ces outils, lorsque c'est possible. En cas de doute, vous pouvez vous renseigner auprès du personnel rattaché à la cybersécurité de votre organisation.

Est-ce crédible?

Privilégiez des outils qui permettent de retracer les opérations ayant mené aux résultats générés par l'IA, afin que vous puissiez les contrevérifier et, dans la mesure du possible, les justifier.

Est-ce bien utilisé?

- Assurez-vous de connaître les limites et les capacités de ces outils avant de vous en servir, car ils évoluent constamment et de nouvelles fonctionnalités apparaissent régulièrement.
- Soyez à l'affût des biais d'utilisation qui émergent, par exemple, quand on utilise toujours le même outil d'IA générative, ou encore dans la manière dont vous formulez vos requêtes Fiche 3.
- Vous devriez vérifier l'information générée par les outils d'IA, en croisant vos sources par exemple.

Est-ce transparent?

Lorsque vous recourez à un outil d'IA générative, informez-en vos collègues ou vos publics, par l'entremise d'un court message ou d'un tatouage numérique.

Pour aller plus loin

Fiche 16

Contribuez à un climat sain dans les débats publics

Ces derniers temps, une nouvelle erronée circule dans les médias sociaux : les données citées ne sont pas sourcées, l'auteur manque de crédibilité, etc. Cependant, il s'avère que cette nouvelle sert votre stratégie de communication publique, et pourrait bien vous aider à convaincre la population de la pertinence des projets de votre organisation. Devriez-vous utiliser cette nouvelle? La dénoncer? L'ignorer?

Si vous êtes porte-parole pour votre organisation ou que vous êtes une personne élue, vous contribuez au débat public, et parfois, vous êtes amené ou amenée à développer des stratégies de communication pour rallier la population à vos idées[78]. Si les débats et la joute politique font intégralement partie de la démocratie, **certains comportements peuvent contribuer, par accumulation, à alimenter le cynisme de la population envers les institutions démocratiques et alimenter la polarisation de la société, dans la sphère numérique comme dans la sphère physique.**

Ces quelques balises contribueront à votre réflexion sur votre responsabilité en tant que porte-parole dans l'espace public[79], afin que nous puissions collectivement offrir à la société québécoise des conditions saines de débat, et ainsi affirmer nos valeurs démocratiques face aux logiques de censure ou d'intimidation exercées dans d'autres États.

- **Il n'est pas éthique de créer des informations qui imitent des personnes,** sans leur consentement (ex. : hypertrucages (*deepfakes*) et autres contenus créés avec l'IA générative) Fiche 15.
- **Vous ne devriez pas reprendre des informations erronées, incomplètes ou non vérifiées** qui sont produites par d'autres, même si celles-ci servent vos intérêts stratégiques.
- **Vous ne devriez pas utiliser les outils d'amplification artificielle** des messages sur les médias sociaux, par exemple ceux impliquant la création de faux comptes.
- **Tentez de vous tenir loin des campagnes de dénigrement des personnes.** Par exemple, évitez d'utiliser des arguments impliquant du salissage, etc.
- **Vous devriez éviter de susciter une peur ou une colère non justifiée envers certaines communautés**. Cela implique, par exemple, d'avoir un recours raisonné à l'émotion comme stratégie de communication Fiche 2.
- **Ayez le souci de protéger les personnes sous-représentées,** qui sont plus susceptibles d'être victimes de propos haineux et de harcèlement[80]. Par exemple, vous devriez éviter de bâtir une argumentation politique découlant de ces caractéristiques, ou encore utiliser de manière responsable les outils de microciblage, qui peuvent augmenter les inégalités et les polarisations entre les communautés[78, 81].
- **Pensez à dénoncer les comportements avérés et non appropriés,** peu importe l'affiliation des personnes impliquées.

Pour aller plus loin

Sous-section 3.2
Actions réactives

Ce que vous pouvez faire lorsque votre institution subit les effets des désordres de l’information.

Fiche 17
Face à la crise : analysez la situation

Un groupe citoyen critique de manière virulente, sur les médias sociaux, le programme phare de votre institution, en citant certaines données hors de leur contexte. Le directeur des affaires publiques débarque dans votre bureau, en criant à la désinformation. En tant que directrice des communications, on vous intime d'agir.

Face à une crise impliquant des informations trompeuses, la première étape consiste à analyser le phénomène dans son contexte, afin de faire preuve de discernement dans des situations complexes, émotives, et pleines d'incertitude. Vous pourrez ensuite décider, de la manière la plus éclairée possible, de la stratégie à adopter Fiche 18.

Six points pour renforcer votre discernement en temps de crise

- **Cherchez d'abord à vérifier ce qui se passe.** Posez des questions aux personnes qui possèdent de l'information (gestionnaire de médias sociaux, direction des communications, sécurité informatique).
- **Méfiez-vous des effets grossissants** générés par la surprise, la couverture médiatique, l'émotion de voir votre organisation affectée, etc.
- **Ramenez la crise à sa juste proportion.** S'étend-elle dans un cercle de personnes convaincues seulement? Est-elle délimitée à un secteur?
- **Résistez à la tentation de présumer que les personnes impliquées sont mal intentionnées.** Ces dernières sont peut-être mal informées.
- **Attention à ne pas confondre les faits et les volontés gouvernementales.** Il est légitime que les volontés gouvernementales fassent l'objet de contestation, mais moins les faits.
- **Prenez en compte le niveau d'incertitude** relié aux informations dont vous disposez.

Pour aller plus loin

Fiche 17
Face à la crise : analysez la situation

Délimitez le désordre informationnel

Sur la base d'un travail de veille ciblée Fiche 10 et de la typologie des désordres de l'information (voir p. 10), tentez de répondre aux questions suivantes :

- En quoi l'information est-elle trompeuse? Tentez de la qualifier.
- Quelle est l'intention affichée des auteurs ou des autrices?
- Peut-on identifier les autrices ou les auteurs? A-t-on affaire à un groupe structuré?
- Quels canaux et quels formats sont utilisés?
- Dans quelle mesure l'information trompeuse est-elle étendue? Dans quelles sphères d'activité, dans quelles communautés?
- Quel est le phénomène social sous-jacent? Essayez de comprendre les origines de la situation, car un désordre de l'information n'émerge jamais de nulle part.

Évaluez les dommages potentiels

- **Sur votre public :** capacité à accéder à vos services, nombre de personnes potentiellement atteintes.
- **Sur la capacité à réaliser votre mission :** effets sur le personnel et sur les services, perte de ressources.
- **Sur votre réputation et sur votre stratégie institutionnelle :** capacité à déployer le plan stratégique, crédibilité de l'institution, image de marque.
- **Sur les autres organisations publiques :** capacité à réaliser leur mission, réputation.
- **Sur la société québécoise :** tensions sociales, perte financière pour l'État, effets sur l'économie, réputation et autonomie du Québec.

En temps de crise, vous ne devriez jamais perdre de vue que votre priorité est d'assurer la sécurité de la population et de préserver le lien de confiance avec les institutions publiques. À ce titre, vous ne devriez pas seulement penser à protéger les intérêts de votre organisation, mais aussi ceux des publics, des autres organisations publiques, et de la société québécoise.

Pour aller plus loin

Fiche 18

Face à la crise : baliser votre plan d'action

La porte-parole de votre organisation veut démentir proactivement des informations erronées qui circulent sur les médias sociaux, parce que celles-ci ont tendance à tromper la population sur ses intentions. Comment la conseiller? D'un côté, vous tenez à adopter des pratiques de communication transparentes… D'un autre côté, vous hésitez à mettre votre organisation sous les projecteurs, ce qui pourrait donner plus de visibilité à l'information erronée.

Pour aller plus loin

Une crise peut être une excellente occasion de renforcer votre capital de confiance, mais peut aussi présenter des risques d'alimenter le cynisme de la population vis-à-vis des institutions publiques. Vous devez donc agir (ou ne pas agir) de manière réfléchie, en vous entourant de spécialistes, et en déployant un plan de sortie de crise, comprenant (ou non!) des actions de communication (ex. : démystification Fiche 19, ou encore des actions légales Fiche 21.

Gardez en tête les principes de communication publique

Ces derniers favorisent l'établissement d'un lien de confiance avec la population, tout en laissant de la place à l'expression du sens critique (voir sous-section Quelques principes de communication publique – p. 36).

Tentez de ne pas nourrir les perceptions qui contribuent à étioler le capital de confiance des institutions publiques.

- **L'État au service des intérêts de ses dirigeants et dirigeantes.** Par exemple, lorsque vous faites du rétablissement de faits Fiche 19, vous pourriez donner l'impression que vous servez des intérêts corporatifs ou partisans avant de servir les intérêts de la population.
- **L'État secret.** Lorsque vous effectuez des actions de promotion uniquement, ou que vous ne communiquez pas toutes les informations sans justification, vous pouvez entretenir le mythe que l'État « nous cache quelque chose », et offrir des prises aux mouvements conspirationnistes.
- **L'État censeur.** Vous ne devriez jamais mener vos interactions dans l'objectif de faire taire des personnes avec vos arguments. Ces dernières pourraient se sentir tenues à l'écart et avoir l'impression que l'État exerce une forme de censure par des arguments d'autorité.
- **L'État prescripteur de la vertu.** Évitez de vous placer comme un arbitre des débats sociaux, au risque de nourrir la perception d'un État moralisateur qui détermine ce qui est juste ou faux, ce qui est bon ou mauvais.

Fiche 18

Face à la crise : baliser votre plan d'action

Associer les personnalités politiques et administratives dans l'espace public? Oui, mais avec prudence!

Bien que les personnalités publiques du milieu politique et administratif puissent collaborer pour communiquer des messages d'intérêt public, surtout en temps de crise, ces dernières n'ont pas le même rôle dans la société. Leur association dans l'espace public ne devrait pas revêtir une dimension partisane, au risque de brouiller la nature de la relation entre la population et ses administrations.

Les lanceurs et lanceuses d'alerte

La protection d'une institution publique ne devrait jamais passer avant la protection du bien commun. Bien que le personnel des institutions publiques soit généralement tenu au devoir de réserve, dans le cas où la sécurité du public est en cause, celui-ci peut être suspendu. C'est pourquoi il est possible pour le personnel de l'État de faire une divulgation au Protecteur du citoyen, à titre de lanceur ou lanceuse d'alerte[82].

Pour aller plus loin

Fiche 19
Démystification et rétablissement de faits

La démystification et le rétablissement de faits sont des campagnes de communication qui permettent de contrer une information trompeuse *a posteriori*, sans tenter d'identifier des coupables, ni leurs intentions. En raison des ressources qu'elles demandent, ces campagnes ne peuvent pas être déployées à grande échelle ou de manière systématique. Elles devraient plutôt être utilisées de manière ciblée, en association avec des mesures préventives[83]. Elles présentent aussi certaines limites et peuvent être moins efficaces avec la montée en puissance des personnalités publiques qui proposent une autre définition de ce qu'on considère être la vérité.

Démystification *(debunking)* et rétablissement de faits *(fact-checking)*

La démystification cible un sujet en particulier, elle constitue une décision stratégique visant à minimiser l'impact d'une information trompeuse. Ex. : un article mentionne que les vaccins causent l'autisme sera démystifié par les autorités de santé publique, afin que la campagne de vaccination puisse suivre son cours.

Le rétablissement de faits est une activité récurrente qui vise à vérifier l'exactitude des faits contenus dans un écrit ou un discours[84]. Ex. : en période électorale, un journaliste vérifie systématiquement les affirmations des candidates et candidats[85].

Une campagne efficace de démystification

- **Devrait suivre les principes de communication publique** (voir sous-section 3), notamment par la production de contenus simples et courts, car les personnes les plus sensibles à la désinformation sont moins susceptibles de trouver les contenus engageants[83, 85].
- **Être déployée seulement quand c'est nécessaire**, pour prévenir un risque notable pour l'institution ou pour le public[83], car elle produit des messages négatifs et donne une certaine visibilité à l'information trompeuse.
- **Impliquer d'autres institutions crédibles auprès des publics visés**[85]. Cela permet de limiter les perceptions du type « L'État prescripteur de la vertu » Fiche 18.

Pour aller plus loin

Fiche 19
Démystification et rétablissement de faits

Composantes essentielles d'une démystification[83]

FAIT	Pour commencer, assurez-vous que le fait soit clair, concis et accrocheur. Rendez-le simple, concret et plausible. Il doit «coller» à l'histoire.
AVERTISSEMENT SUR LE MYTHE	Prévenir à l'avance de la présence d'un mythe... ne le mentionnez qu'une seule fois.
EXPLIQUER LE FAUX RAISONNEMENT	Expliquer comment le mythe induit en erreur.
FAIT	Terminez en renforçant le fait - plusieurs fois si possible. Veillez à proposer une alternative à l'explication causale.

Pour aller plus loin

Fiche 20
Leviers juridiques reliés aux désordres de l'information

Vous disposez de plusieurs leviers juridiques pour pallier les effets des désordres de l'information, lorsque vous ou votre organisation subissez des préjudices qui vous empêchent de réaliser pleinement votre mission. Ces leviers sont balisés par le principe de liberté d'expression, inscrite dans la *Charte canadienne des droits et libertés* et dans la *Charte des droits et libertés de la personne du Québec*.

Quelques leviers juridiques

En invoquant les recours suivants devant la justice, vous pourriez obtenir des dommages et intérêts, le retrait de publications, ou la publication de rectificatifs. Certains recours permettent aussi des condamnations pénales.

Diffamation[86]. Propagation d'une information fausse et nuisible à l'honneur ou à la réputation d'une personne ou d'une organisation.
Ex. : en 2009, un groupe citoyen d'une ville québécoise a été condamné pour avoir traité la mairesse de la ville de « maire SS », de « paranoïaque profonde » et de « *bitch* » sur un forum de discussion[87].

Atteinte à la vie privée[86]. Divulgation non autorisée d'informations personnelles et privées qui porte atteinte à la vie privée d'une personne.
Ex. : on peut s'exposer à une condamnation si on dévoile l'adresse privée d'une personne élue dans les médias sociaux.

Diffamation dans un contexte de débat public : où est la limite[90]?

Il pourrait y avoir diffamation dans les cas suivants :

- Lorsqu'on prononce des propos désagréables à l'égard d'une personne tout en les sachant faux.
- Lorsqu'on diffuse des propos désagréables sur une personne alors qu'on devrait les savoir faux.
- Lorsqu'on tient des propos défavorables, mais véridiques, à l'égard d'une personne, mais sans justes motifs (ex. : il n'est pas dans l'intérêt public de connaître cette information).

Pour aller plus loin

Fiche 20
Leviers juridiques reliés aux désordres de l'information

Incitation à la violence[88]. Il est illégal de formuler des menaces, des intimidations et des appels à la violence ou à la haine envers une personne ou un groupe identifiable. Ex. : on ne peut pas appeler à vandaliser les biens d'une personne à la tête d'une société d'État parce qu'on est en désaccord avec ses décisions.

Harcèlement[89]**.** Le harcèlement se manifeste par des paroles ou des comportements offensants, méprisants, hostiles ou non désirés. Ex. : le directeur général d'une municipalité reçoit des messages texte répétés de la part d'un citoyen insatisfait, qui le menace de vandaliser son automobile et sa maison.

Usurpation d'identité[88]**.** Se faire passer pour une autre personne ou commettre une fraude en utilisant des informations personnelles appartenant à une autre personne sans son consentement. Ex. : ouvrir un compte X au nom d'une personnalité publique, sans son accord.

Utilisation frauduleuse d'une identité visuelle[91]**.** Ex. : utiliser le logo d'un ministère dans un message publié sur les médias sociaux, afin de donner plus de crédibilité à ce dernier.

Manquement à l'obligation de retrait[86]**.** La loi stipule qu'une personne doit réparer les dommages causés à autrui par sa faute. Ex. : si une plateforme médiatique a été informée qu'un contenu est illicite et qu'elle ne prend pas de mesures pour le retirer, elle est tenue de dédommager la personne lésée, au même titre que l'auteur ou l'autrice.

AVERTISSEMENT : cette fiche ne constitue pas, en tant que telle, un conseil juridique. Plusieurs éléments spécifiques à votre cas doivent être pris en considération, avec l'aide de spécialistes en droit **Fiche 21****.**

Renfort juridique pour les municipalités

La nouvelle *Loi visant à protéger les élus municipaux et à favoriser l'exercice sans entraves de leurs fonctions (LPEM)* prévoit de nouvelles infractions pénales permettant maintenant de sanctionner toute personne qui entrave l'exercice de la fonction d'une élue ou d'un élu municipal en le menaçant, en l'intimidant ou en le harcelant ou en troublant le déroulement d'une séance du conseil d'un organisme municipal.

Pour aller plus loin

Fiche 21

Actions en justice : comment procéder?

Un compte sur la plateforme X, reprenant la facture visuelle du gouvernement du Québec, diffuse des communiqués erronés annonçant l'abolition du programme de crédit d'impôt pour soutien aux personnes aînées, puis l'arrêt du supplément pour personne en situation de handicap. Certains médias ont été bernés et ont partagé la nouvelle. Les lignes téléphoniques des ministères concernés sont débordées par des centaines d'appels de personnes inquiètes.

Il est parfois incontournable d'intenter une action en justice, comme dans la situation décrite précédemment. Mais cela demande du temps et des ressources, et peut entraîner des contre-effets dommageables, il convient donc de bien réfléchir avant de s'y engager Fiche 18.

Documentez le préjudice

Dès que la situation se présente, recueillez des preuves : enregistrez les pages en format HTML (à défaut, prenez des saisies d'écran), et prenez en note toutes les informations sur le préjudice et ses circonstances, dans les limites du respect de la vie privée. Documentez aussi les conséquences du préjudice sur votre personnel, les publics, votre capacité à réaliser votre mission, etc.

Sollicitez le soutien approprié

En tant que titulaire de charge publique, il est d'usage que vous meniez une action en justice en rapport avec votre travail, avec le soutien de l'organisation à laquelle vous appartenez.

- **Pour un élu ou une élue du gouvernement du Québec** (y compris les ministres), c'est l'Assemblée nationale du Québec.
- **Pour un élu ou une élue d'une municipalité,** c'est la direction juridique de la municipalité. Les organisations municipales mettent à disposition des municipalités certaines ressources d'aide.
- **Pour une personne titulaire d'un emploi dans un ministère ou un organisme public,** c'est la direction des affaires juridiques de cet organisme, qui est elle-même reliée au ministère de la Justice.
- **Pour une personne titulaire d'un emploi supérieur** nommée par le Conseil des ministres, c'est le Secrétariat aux Emplois supérieurs.

Cependant, vous pouvez aussi entamer des poursuites en tant que personne privée.

Pour aller plus loin

Fiche 21
Actions en justice : comment procéder?

Élaborez votre stratégie, avec une personne qualifiée en droit

Selon votre situation spécifique, cette stratégie peut comprendre :

- L'évaluation des leviers juridiques qui pourraient être utilisés Fiche 20.
- Une tentative de règlement par la médiation et le dialogue, par exemple en demandant la rectification ou le retrait d'un contenu sur les médias sociaux.
- Le dépôt d'une plainte à la police ou devant les tribunaux civils ou administratifs, ou encore à la Commission municipale du Québec[80, 92].
- L'obtention d'une protection particulière, comme une injonction ou une ordonnance, ou une protection policière si vous avez reçu des menaces crédibles de violence ou de cyberharcèlement.

Pour aller plus loin

Section 4
Conclusion

Conclusion

Notre rapport à la réalité a complètement changé. L'influence des données probantes, de la science et des institutions n'est plus la même dans la société[93]. Les institutions publiques doivent nécessairement évoluer au regard de ces transformations, afin de demeurer des organisations de référence pour la population, et entretenir un lien de confiance qui ne se présente plus comme un acquis. Aujourd'hui vous ne devriez plus vous attendre à ce que les Québécoises et les Québécois aient aveuglément confiance dans leurs institutions, c'est pourquoi vous devriez agir de telle sorte que toutes et tous puissent contribuer aux débats publics, poser des questions, exercer leur sens critique et faire partie des solutions.

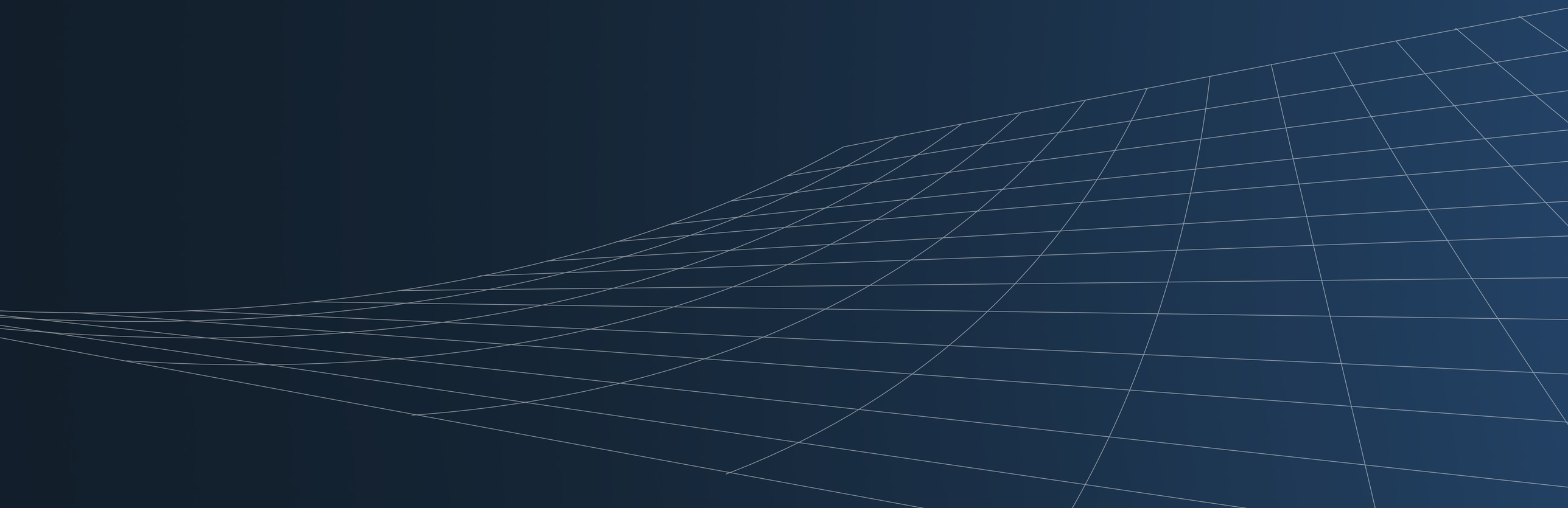
Après avoir lu ce guide, en tout ou en partie, vous saisissez peut-être davantage la nature de vos responsabilités dans les désordres de l'information. Votre position, qui est celle de servir le bien commun sur la base de données probantes, n'est aujourd'hui plus totalement neutre dans l'ordre géopolitique mondial. Elle constitue en soi **un engagement pour préserver les acquis démocratiques du Québec, contre l'influence des pensées extrémistes et autoritaires, issues des États-Unis notamment.** Votre contribution devient aujourd'hui plus essentielle que jamais.

Vous aurez trouvé dans ce guide plusieurs pistes d'action, et il vous semblera peut-être difficile de toutes les appliquer dans votre quotidien. Il n'y a que 24 heures dans une journée, et **vous devrez nécessairement demeurer humbles face à ces désordres de l'information, en collaborant avec d'autres.** Autour de vous, plusieurs collègues disposent d'expériences et d'expertises différentes. Vous ne devriez jamais hésiter à avoir recours à ces personnes. Tout comme vous, d'autres acteurs et actrices au Québec portent cette responsabilité collective, comme les entreprises, les médias d'information, les parents, et les citoyennes et les citoyens. Enfin, vous pouvez compter sur la communauté scientifique pour mobiliser les informations scientifiques dont vous avez besoin, et documenter ces désordres de l'information dans toute leur complexité.

Nous devons plus que jamais nous engager collectivement pour préserver nos acquis démocratiques, renforcer notre résilience collective face aux désordres de l'information, et ainsi maintenir notre souveraineté gouvernementale.

Section 5
Pour aller plus loin

Des ressources pour approfondir vos connaissances :
guides, formations, sites Web de références, à partager avec vos équipes.



Pour aller plus loin

Fiche 1 – Quelques techniques pour tromper les internautes

Repérer les « bots » ou les faux comptes sur les médias sociaux – Les Décrypteurs

Petit guide pour repérer les « bots » – La science d'abord

Fiches 3 et 4 – Les défauts de notre cerveau

Codex complet des biais cognitifs

Il faut se méfier de nos raccourcis mentaux – Agence Science Presse

Pharmachien – La bible des arguments qui n'ont pas d'allure – Olivier Bernard

Fiche 5 – Cette nouvelle sur le Web est-elle fiable?

Êtes-vous en mesure de détecter les fausses informations sur le web? Les Décrypteurs

Fiche 6 – Confirmer la véracité d'une image ou d'une vidéo

Recherche de sources d'images – Tiny Eye

La vérité derrière une photo – Les Décrypteurs

Repérer les vidéos manipulées – Les Décrypteurs

Fiche 8 – Évaluez la valeur d'une information scientifique

Initiative canadienne de lutte à la désinformation par la science – LaSciencedAbord

Formation Décoder l'information scientifique – Agence Science-Presse

Fiche 9 – Comment se porte votre empreinte numérique?

Conseils en cybersécurité – Gouvernement du Québec

Apprenez à protéger votre information et vos données lorsque vous utilisez des applications – Gouvernement du Canada

Ce qu'il faut savoir sur les *cookies* Internet – Gouvernement du Canada

Quelques principes de communication publique

Système de design gouvernemental – Gouvernement du Québec

Bonnes pratiques numériques gouvernementales – Gouvernement du Québec

Fiche 10 – Veille ciblée : déployez vos antennes

Répertoire des outils de veille – Réseau stratégique de veille et de prospective

Conseils sur la confidentialité des navigateurs Internet : Paramètres du navigateur – Sécurité technologique Canada

Pour aller plus loin

Fiche 11 – Évaluez les risques d'opérations d'influence

L'ingérence étrangère et vous – Gouvernement du Canada

Guide de sensibilisation sur la sécurité de l'information – Gouvernement du Québec

Fiche 12 – Configurez les médias sociaux

Utilisation de comptes personnels de médias sociaux au travail – Gouvernement du Canada

Perte de contrôle des comptes de médias sociaux – Gouvernement du Canada

Parlementaires : signalez les faux comptes de médias sociaux – Gouvernement du Canada

Fiche 13 – Animez les espaces de dialogue

Exemple de nétiquette – Ville de Québec

Exemple de nétiquette – ministère de la Cybersécurité et du Numérique – Gouvernement du Québec

Bonnes pratiques pour contrer le cyberharcèlement – ministère des Affaires municipales et de l'Habitation – Gouvernement du Québec

Fiche 14 – Mieux vaut prévenir que guérir… l'inoculation

Fiches pédagogiques – Centre québécois d'éducation aux médias

Ressources en littératie numérique et éducation aux médias – HabiloMédias

Formations – Agence Science-Presse

Fiche 15 – Utilisation responsable de l'intelligence artificielle (IA) générative

Guide de bonnes pratiques d'utilisation de l'IA générative – ministère de la Cybersécurité et du Numérique – Gouvernement du Québec

Guide pratique d'utilisation de l'IA générative pour les municipalités du Québec – Obvia

Enjeux sociétaux de l'IA 101 : un guide pour démystifier les enjeux éthiques et juridiques des systèmes d'IA – Obvia

Pour aller plus loin

Fiche 19 – Démystification et vérification de faits

International Fact-Checking Network

Le Détecteur de rumeurs – Agence Science-Presse

Les Décrypteurs – Radio-Canada

Fiche 20 – Leviers juridiques reliés aux désordres de l'information

Loi visant à protéger les élus municipaux et à favoriser l'exercice sans entraves de leurs fonctions et modifiant diverses dispositions législatives concernant le domaine municipal

Fiche 21 – Actions en justice : comment procéder

Intimidation et harcèlement des élus·es – Fédération québécoise des municipalités

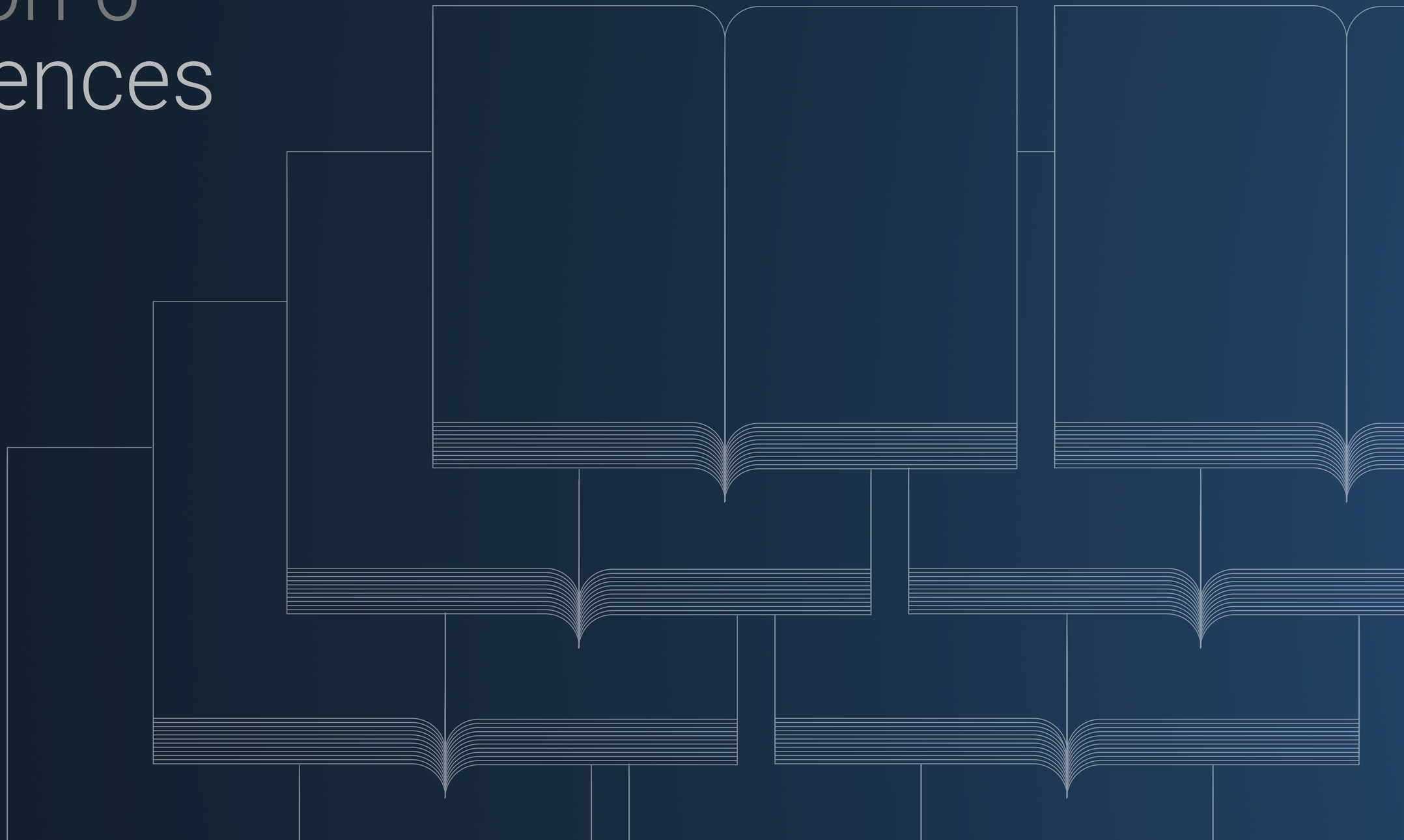
Programme d'aide aux élu(e)s et à leur famille immédiate – Fédération québécoise des municipalités

Plan de lutte contre l'intimidation – Sureté du Québec

Fonds municipal d'action juridique (volet harcèlement) – Union des municipalités du Québec

Liens consultés le 22 septembre 2025.

Section 6
Références



Références

1. LESHER, M., PAWELEC, H. et DESAI, A. (2022). ***Disentangling untruths online: Creators, spreaders and how to stop them*, OECD Going Digital Toolkit Notes, Nº 23, OECD Publishing.** https://doi.org/10.1787/84b62df1-en
2. WARDLE, C. (2019). ***Understanding Information Disorder,* First Draft.** https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x21167
3. BATEMAN, J. et JACKSON, D. (2024). ***Countering Disinformation Effectively: An Evidence-Based Policy Guide,* Carnegie Endowment for International Peace.** https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en
4. LOBBYISME QUÉBEC (s. d.). ***Types de titulaires de charge publique.*** https://lobbyisme.quebec/titulaire-dune-charge-publique/types-de-titulaires-de-charges-publiques/
5. COMMISSION BRONNER (2022). ***Les Lumières à l'ère numérique, rapport de la Commission.*** https://documentation.insp.gouv.fr/insp/doc/SYRACUSE/394350/les-lumieres-a-l-ere-numerique-rapport-de-la-commission-gerald-bronner-roland-cayrol-laurent-cordoni?_lg=fr-FR#:~:text=Le%20rapport%20%C3%A9tablit%20de%20mani%C3%A8re%20synth%C3%A9tique%20l%E2%80%99%C3%A9tat%20des,et%20formule%20des%20recommandations%20pour%20y%20faire%20face.
6. UK GOVERNMENT COMMUNICATION SERVICE (2021). ***Resist 2, Counter Disinformation Toolkit*.** https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/
7. BUREAU DU CONSEIL PRIVÉ (2024). ***Lutter contre la désinformation : guide à l'intention des fonctionnaires*.** https://www.canada.ca/fr/institutions-democratiques/services/proteger-institutions-democratiques/lutter-contre-desinformation-guide-intention-fonctionnaires.html
8. JACK, C. (2017). ***Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute.** https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf
9. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (2024). ***Les faits sans le faux : lutter contre la désinformation, renforcer l'intégrité de l'information,* Éditions OCDE.** https://doi.org/10.1787/4078bb32-fr
10. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (2011). ***Média social,* Grand dictionnaire terminologique.** https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26502881/media-social
11. COUTANT, A. et STENGER, T. (2012). ***Les médias sociaux : une histoire de participation*, Le Temps des médias, 18(1), 76-86.** https://doi.org/10.3917/tdm.018.0076
12. UK DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY (2025). ***International AI Safety Report,* AI Action Summit.** https://www.gov.uk/government/publications/international-ai-safety-report-2025/international-ai-safety-report-2025#current-capabilities
13. SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (2025). ***Défis et « opportunités » de l'intelligence artificielle dans la lutte contre les manipulations de l'information,* Sommet pour l'Action sur l'IA.** https://www.sgdsn.gouv.fr/publications/defis-et-opportunites-de-lintelligence-artificielle-dans-la-lutte-contre-les
14. ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE (2024). ***Intelligence artificielle générative et données personnelles,* NETendances 2024, vol. 15, nº 5.** https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/intelligence-artificielle-generative-et-donnees-personnelles-2024/
15. CONSEIL DE L'INNOVATION DU QUÉBEC (2024). ***Prêt pour l'IA. Répondre au défi du développement et du déploiement responsables de l'IA au Québec.*** https://conseilinnovation.quebec/wp-content/uploads/2024/02/Rapport_IA_CIQ-1.pdf
16. CENTRE DE LA CYBERSÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (2025). ***Cybermenaces contre le processus démocratique du Canada. Mise à jour de 2025.*** https://www.cyber.gc.ca/sites/default/files/tdp-2025-f-v1_0.pdf
17. HASSAN, G., BROUILLETTE-ALARIE, S., SÉRAPHIN, A., FRAU-MEIGS, D., LAVOIE, L., FETIU, A., VARELA, W., BOROKHOVSKI, E., VENKATESH, V., ROUSSEAU, C. et SIECKELINCK, S. (2018). ***Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence,* International Journal of Developmental Sciences, 12, 1-18.** https://doi.org/10.3233/DEV-170233
18. CARIGNAN, M.-E., MORIN, D., DAXHELET, M.-L., BÉDARD, S., CHAMPAGNE-POIRIER, O., CHOQUETTE, E., ALIAGA, G., KENNACHE, Y. et KAMELA, E. K. (2022). ***Le mouvement conspirationniste au Québec : leaders, discours et adhésion,* Chaire UNESCO en prévention de la radicalisation et de l'extrémisme violents.** https://chaireunesco-prev.ca/wp-content/uploads/2022/06/UNESCO-PREV_RapportRecherche_MEI_final.pdf

Références

19. GROUPE DE RECHERCHE SUR LA COMMUNICATION MARKETING CLIMATIQUE (2024). ***Baromètre de l'action climatique : Disposition des Québécoises et Québécois envers les défis climatiques.*** https://cdn.prod.website-files.com/65de237a907486cd99c45264/6751cde275af0d688f16b19c_BarometreClimat2024_WEB_compressed.pdf

20. BÉDARD, S., CARIGNAN, M.-E. et autres (2025). ***Désinformation et déni climatique : revue de la littérature et portrait de la situation au Québec.*** **Chaire UNESCO en prévention de la radicalisation et de l'extrémisme violents.** https://chaireunesco-prev.ca/rapport-desinformation-et-deni-climatique-revue-de-la-litterature-et-portrait-de-la-situation-au-quebec/

21. CONSEIL DES ACADÉMIES CANADIENNES (2023). ***Lignes de faille. Comité d'experts sur les conséquences socio-économiques de la mésinformation en science et en santé.*** https://www.rapports-cac.ca/reports/les-consequences-socio-economiques-de-la-mesinformation-en-science-et-en-sante/

22. RICHARD, G., GRAINDORGE, A., CHARBONNEAU, A., VALLERAND, O. et HOUZEAU, M. (2025). ***Augmentation des niveaux de malaise. Ce que les élèves du secondaire pensent de la diversité sexuelle, 2017-2024.*** **GRIS-Montréal.** https://www.gris.ca/app/uploads/2025/01/GRIS_rapport-final_30jan2025.pdf

23. TANNER, S. et GILLARDIN, F. (2025). ***Toxic Communication on TikTok: Sigma Masculinities and Gendered Disinformation,*** **Social Media + Society, 11(1).** https://journals.sagepub.com/doi/10.1177/20563051251313844

24. OUATIK, B. (2020). ***Non, le coronavirus n'a pas été créé à partir du VIH*****, Radio-Canada.** https://ici.radio-canada.ca/nouvelle/1695718/coronavirus-sras-cov2-vih-sequence-luc-montagnier-faux

25. MELOCHE-HOLUBOWSKI, M. (2024). ***Faux remède contre la COVID-19 : Didier Raoult interdit de pratiquer pour 2 ans,*** **Radio-Canada.** https://ici.radio-canada.ca/nouvelle/2110730/didier-raoult-hydroxychloroquine-sanction

26. CLICHE, J.-F. (2025). ***La première suspension de Patrick Provost réduite de moitié*****, le Soleil.** https://www.lesoleil.com/science/2025/04/03/la-premiere-suspension-de-patrick-provost-reduite-de-moitie-NTMDGDJSGRGRPG4B7BHFTZEEHE/

27. BRIDGMAN, A., LAVIGNE, M., BAKER, M., BERGERON, T., BOHONOS, D., BURTON, A., McCOY, K., HART, M., LAVAULT, M., LIDDAR, R., PENG, P., ROSS, C., VICTOR, J., OWEN, T. et LOEWEN, P. (2022). ***Mis- and Disinformation During the 2021 Canadian Federal Election,*** **Media Ecosystem Observatory.** https://meo.ca/work/election-misinfo/canada2021

28. MATASICK, C., ALFONSI, C. et BELLANTONI, A. (2020). ***Les mesures de gouvernance publique face à la désinformation : comment les principes de gouvernement ouvert peuvent éclairer les choix stratégiques,*** **nº 39, Éditions OCDE.** https://doi.org/10.1787/a4000a8c-fr

29. EARNSHAW, V.A., EATON, L.A., KALICHMAN, S.C., BROUSSEAU, N.M., HILL, E.C. et FOX, A.B. (2020). ***COVID-19 conspiracy beliefs, health behaviors, and policy support,*** **10(4), 850-856.** https://doi.org/10.1093/tbm/ibaa090

30. FREEMAN, D., WAITE, F., ROSEBROCK, L., PETIT, A., CAUSIER, C., EAST, A., JENNER, L., TEALE, A.L., CARR, L., MULHALL, S., BOLD, E. et LAMBE, S. (2022). ***Coronavirus conspiracy beliefs, mistrust, and compliance with government guidelines in England, Psychological Medicine,*** **52(2), 251-263.** https://doi.org/10.1017/S0033291720001890

31. DE CONINCK, D., FRISSEN, T., MATTHIJS, K., D'HAENENS, L., LITS, G., CHAMPAGNE-POIRIER, O., CARIGNAN, M.-E., DAVID, M.-D., PIGNARD-CHEYNEL, N., SALERNO, S. et GÉNÉREUX, M. (2021). ***Beliefs in Conspiracy Theories and Misinformation About COVID-19: Comparative Perspectives on the Role of Anxiety, Depression and Exposure to and Trust in Information Sources,*** **Frontiers in Psychology, vol. 12, 646394.** https://doi.org/10.3389/fpsyg.2021.646394

32. NEWMAN, N. (2025). ***Digital News Report 2025,*** **Reuters Institute.** https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025

33. CENTRE D'ÉTUDE SUR LES MÉDIAS (2024). ***Digital News Report 2025 — synthèse des données canadiennes.*** https://www.cem.ulaval.ca/wp-content/uploads/2025/06/dnrcanada2025f.pdf

34. EDELMAN (2025). ***Baromètre de confiance Edelman 2025 – Québec,*** **Edelman Trust Institute.** https://www.edelman.com/ca/fr/trust/2025/trust-barometer

35. DFRLAB (2017). ***#BotSpot: Twelve Ways to Spot a Bo*****t, Medium.** https://medium.com/dfrlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c

36. CAULFIELD, M. (2017). ***Web Literacy for Student Fact-Checkers,*** **Pressbooks, en ligne** https://pressbooks.pub/webliteracy/

37. PROULX, S. (2018). L'accusation de *fake news* : médias sociaux et effets politiques. Dans SAUVAGEAU, F., THIBAULT, S. et TRUDEL, P. (Eds.), ***Les fausses nouvelles, nouveaux visages, nouveaux défis. Comment déterminer la valeur de l'information dans les sociétés démocratiques?*** (p. 63-78). Presses de l'Université Laval.

Références

38. WOLLEBÆK, D., KARLSEN, R., STEEN-JOHNSEN, K., et ENJOLRAS, B. (2019). ***Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior.*** **Social media + society, 5(2).** https://doi.org/10.1177/2056305119829859

39. KAHNEMAN, D. (2011). ***Thinking, Fast and Slow*** **(1st ed), Farrar, Straus and Giroux.**

40. MANOOGIAN, J. III et BENSON, B. (s. d.). ***Cognitive bias codex, traduit.*** https://inertian.wixsite.com/codexbiais

41. COOK, J. (2020). ***A history of FLICC: the 5 techniques of science denial.*** https://skepticalscience.com/history-flicc-5-techniques-science-denial.html

42. BERNARD, O. (2017). ***La bible des arguments qui n'ont pas d'allure.***

43. PARIS, B. et DONOVAN, J. (2019). ***Deepfakes and Cheap Fakes, The Manipulation of Audio and Visual Evidence,*** **Data and Society.** https://datasociety.net/library/deepfakes-and-cheap-fakes/

44. LACHAPELLE, R. (2022). ***Peut-on déjouer les algorithmes?*** **CQÉMI** https://www.cqemi.org/fr/articles-details-1/peut-on-dejouer-les-algorithmes

45. YATES, J. (2017). ***J'ai testé les algorithmes de Facebook et ça a rapidement dégénéré,*** **Radio-Canada.** https://ici.radio-canada.ca/nouvelle/1029916/experience-facebook-algorithmes-bulle-desinformation

46. AGENCE SCIENCE-PRESSE (2020). ***Qu'est-ce qu'un consensus scientifique?*** https://www.sciencepresse.qc.ca/actualite/covid-19-depister-desinfo/2020/10/23/consensus-scientifique

47. VADEBONCOEUR, A. (2015). ***Le salami, votre ennemi?*** **Tout est relatif!, L'actualité.** https://lactualite.com/sante-et-science/le-salami-votre-ennemi-tout-est-relatif/

48. UNTERSINGER, M. (2024). ***Strava, une histoire émaillée de failles de sécurité,*** **Le Monde.** https://www.lemonde.fr/pixels/article/2024/10/27/strava-une-histoire-emaillee-de-failles-de-securite_6361676_4408996.html

49. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ (2024). ***Empreinte numérique.*** **Série sensibilisation. Centre de la sécurité des télécommunications.** https://www.cyber.gc.ca/fr/orientation/empreinte-numerique-itsap00133

50. BOURDON, S., SCHIRER, A. et CELLULE ENQUÊTE VIDÉO (2024). ***La sécurité de Macron, Biden et Poutine compromise par leurs gardes du corps : le premier épisode de notre enquête « StravaLeaks »,*** **Le Monde.** https://www.lemonde.fr/societe/article/2024/10/27/comment-suivre-a-la-trace-emmanuel-macron-decouvrez-le-premier-episode-de-notre-enquete-stravaleaks_6361677_3224.html

51. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2023). ***Good practice principles for public communication responses to mis- and disinformation*****, OECD public governance policy papers, N° 30, OECD publishing.** https://doi.org/10.1787/6d141b44-en

52. NORRIS, P. (2022). ***In Praise of Skepticism: Trust but Verify*****, Oxford University Press.** https://doi.org/10.1093/oso/9780197530108.001.0001

53. GOUVERNEMENT DU QUÉBEC (s. d.). **Principes de design | système de design gouvernemental.** https://design.quebec.ca/a-propos/fondements/principes-design

54. BARTLEMAN, M. et DUBOIS, E. (2024). ***Les utilisations politiques de l'IA au Canada.*** **Labo Pol Comm Tech, Université d'Ottawa.** http://fr.polcommtech.com/aipolitics-report

55. CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE (s. d.). ***Classification de sécurité des données numériques gouvernementales.*** https://www.cyber.gouv.qc.ca/services/classification-securite-donnees-numeriques-gouvernementales

56. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ (2024). ***Évaluation des cybermenaces nationales 2025-2026,*** **Centre de la sécurité des télécommunications Canada.** https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

57. MINISTÈRE DE L'ÉNERGIE ET DES RESSOURCES NATURELLES (2020). ***Les minéraux critiques et stratégiques, plan québécois pour la valorisation des minéraux critiques et stratégiques 2020-2025,*** **gouvernement du Québec.** https://www.quebec.ca/gouvernement/politiques-orientations/plan-quebecois-valorisation-mineraux-critiques-strategiques

58. MINISTÈRE DE L'INNOVATION, DES SCIENCES ET DU DÉVELOPPEMENT ÉCONOMIQUE (2023). ***Domaines de recherche en technologies sensibles,*** **gouvernement du Canada.** https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/recherche-technologies-sensibles-affiliations-preoccupantes/domaines-recherche-technologies-sensibles

Références

59. SÉCURITÉ PUBLIQUE CANADA (2023). ***Accroître la transparence en matière d'influence étrangère : examiner les mesures pour renforcer l'approche du Canada,*** **gouvernement du Canada.** https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-fr.aspx

60. COMITÉ DES PARLEMENTAIRES SUR LA SÉCURITÉ NATIONALE ET LE RENSEIGNEMENT (2024). ***Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada*** **(version révisée en application du paragraphe 21(5) de la loi sur le CPSNR), gouvernement du Canada.** https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/intro-fr.html

61. SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (2021a). ***Menaces d'ingérence étrangère visant les processus démocratiques du Canada,*** **gouvernement du Canada.** https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/menace-dingerence-etrangere-visant-les-processus-democratiques-du-canada.html

62. SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (2021b). ***L'ingérence étrangère et vous,*** **gouvernement du Canada.** https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-and-you/AOSE_ForeignInterferenceHandout_FR%20-%20Digital_ISBN_A.pdf

63. SECRÉTARIAT DU CONSEIL DU TRÉSOR (2021). ***Directive gouvernementale sur la sécurité de l'information,*** **gouvernement du Québec.** https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/directive_securite_information2021.pdf

64. AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE (2025). ***Science diplomacy in an era of disruption***. https://www.aaas.org/sites/default/files/2025-02/Final_Science%20diplomacy_15%20years%20on_report_WEB.pdf

65. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ (2022). ***Facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation,*** **gouvernement du Canada.** https://www.cyber.gc.ca/sites/default/files/cyber/2022-01/ITSM-10-066-Security-considerations-when-using-social-media-in-your-organization_f.pdf

66. SECRÉTARIAT DU CONSEIL DU TRÉSOR (2025). ***Les enjeux éthiques de l'utilisation des médias sociaux par le personnel des organisations publiques,*** **Formation à l'intention du personnel de la fonction publique, Direction de la santé des personnes et de l'éthique, document interne.**

67. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA. ***Lignes directrices pour les fonctionnaires concernant l'utilisation personnelle des médias sociaux*** **(s. d.) .** https://www.canada.ca/fr/secretariat-conseil-tresor/sujets/valeurs-ethique/lignes-directrices-pour-les-fonctionnaires-utilisation-personnelle-medias-sociaux.html

68. **QUÉBEC. F-3.1.1 - Loi sur la fonction publique.** https://www.legisquebec.gouv.qc.ca/fr/document/lc/F-3.1.1

69. **QUÉBEC. F-3.1.1, r. 3 - Règlement sur l'éthique et la discipline dans la fonction publique.** https://www.legisquebec.gouv.qc.ca/fr/document/rc/F-3.1.1%2C%20r.%203%20/

70. PAYEN, M. (2017). ***Pompier suspendu pour ses propos sur Facebook***, **Journal de Montréal.** https://www.journaldemontreal.com/2017/06/26/pompier-suspendu-pour-ses-propos-sur-facebook

71. MINISTÈRE DES AFFAIRES MUNICIPALES DE L'HABITATION (s. d.). ***Contrer le cyberharcèlement en politique municipale : les bonnes pratiques à adopter,*** **gouvernement du Québec.** https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/affaires-municipales/publications/elections/BRO_Feuillet_MediasSociaux.pdf

72. GARCIA, L. et SHANE, T. (2021). ***A guide to prebunking: a promising way to inoculate against misinformation*****, First Draft.** https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/

73. ROOZENBEEK J., VAN DER LINDEN, S., GOLDBERG, B., RATHJE, S. et LEWANDOSKY S. (2022). ***Psychological inoculation improves resilience against misinformation on social media,*** **Science Advances, 8(34), eabo6254.** https://doi.org/10.1126/sciadv.abo6254

74. PENNYCOOK, G., RAND, D.G. (2022). ***Accuracy prompts are a replicable and generalizable approach for reducing the spread of misinformation,*** **Nature Communications, 13, 2333.** https://doi.Org/10.1038/s41467-022-30073-5

75. GOUVERNEMENT DU QUÉBEC (2021). ***Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026.*** https://www.quebec.ca/gouvernement/politiques-orientations/strategie-integration-ia-administration-publique-2021-2026

Références

76. MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE (2024). *Guide des bonnes pratiques d'utilisation de l'intelligence artificielle générative applicable aux outils d'intelligence artificielle générative externes,* gouvernement du Québec. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/Strategie_cybersecurite_numerique_2024-2028/GU_bonnes_pratiques_utilisation_IA_generative_VF.pdf

77. OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE (2024). *Pourquoi la sobriété numérique? Dans l'œil de l'Obvia*. https://www.obvia.ca/sites/obvia.ca/files/ressources/202412-OBV-Pub-DansIOeildelObvia_Dec2024.pdf

78. DUBOIS, P. (2024). *La communication publique (micro)ciblée : enjeux et réflexions pour la pratique,* ÉNAP, *A+ international,* nº 10. https://espace.enap.ca/id/eprint/500/1/Dubois_Communication_publique_20240425.pdf

79. TRANSATLANTIC COMMISSION ON ELECTION INTEGRITY (s. d.). *The Pledge for Election Integrity* https://www.electionpledge.eu/

80. LALANCETTE, M. (2023). L*a gestion par les élues et élus municipaux des actes et propos violents, haineux ou déplacés à leur égard,* rapport de recherche adressé à madame Andrée Laforest, ministre des Affaires municipales et de l'habitation (MAMH) du Québec. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/affaires-municipales/publications/organisation_municipale/democratie_municipale/RAP_gestion_elus_municipaux_actes_violents.pdf

81. ÉLECTIONS QUÉBEC (2024). *Pour une nouvelle vision de la Loi électorale.* Rapport de recommandations. Directeur général des élections du Québec. https://docs.electionsquebec.qc.ca/ORG/673f441481a7b/DGE-6329.pdf

82. CEVA, E. (2020). *Justice et corruption politique : une justification du devoir de lancer l'alerte,* Raisons politiques, n° 80(4), 59-76. https://doi.org/10.3917/rai.080.0059

83. LEWANDOWSKY, S., COOK, J., ECKER, U. K. H., ALBARRACÍN, D., AMAZEEN, M. A., KENDEOU, P., LOMBARDI, D., NEWMAN, E. J., PENNYCOOK, G., PORTER, E., RAND, D. G., RAPP, D. N., REIFLER, J., ROOZENBEEK, J., SCHMID, P., SEIFERT, C. M., SINATRA, G. M., SWIRE-THOMPSON, B., VAN DER LINDEN, S., VRAGA, E. K., WOOD, T. J., ZARAGOZA, M. S. (2020). *Le Manuel de Démystification 2020*. https://skepticalscience.com/docs/DebunkingHandbook2020-French.pdf

84. DAUPHIN F. (2023). *Le debunking sur YouTube : une nouvelle pratique de lutte contre la désinformation en marge du journalisme,* Les enjeux de l'information et de la communication, nº 23/1A S1, 31-45. https://doi.org/10.3917/enic.Hs13.0031

85. PAMMENT, J., et KIMBER LINDWALL, A. (2021). *Fact-checking and Debunking,* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/fact-checking-and-debunking/8

86. QUÉBEC. Loi concernant le cadre juridique des technologies de l'information RLRQ C-1.1 (2001). https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-1.1

87. LACOURSIÈRE, A. (2009) Un frein à l'intimidation sur l'internet, La Presse. https://www.lapresse.ca/actualites/quebec-canada/justice-et-faits-divers/200907/14/01-884148-un-frein-a-lintimidation-sur-linternet.php

88. CANADA. Code criminel (L.R.C. (1985), ch. C-46). https://laws-lois.justice.gc.ca/fra/lois/c-46/

89. QUÉBEC. Charte des droits et libertés de la personne, RLRQ. C.12 (1975). https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-12

90. Décision Prud'homme c. Prud'homme, [2002] 4 RCS 663 de la Cour Suprême. https://canlii.ca/t/1g2w4

91. CANADA. Loi sur les marques de commerce (L.R.C. (1985), ch. T-13). https://laws-lois.justice.gc.ca/fra/lois/t-13/

92. COMMISSION MUNICIPALE QUÉBEC (s. d.). Enquêtes et poursuites le mandat. https://www.cmq.gouv.qc.ca/fr/enquetes-et-poursuites

93. LARSON, H. J. et BERSOFF, D. M. (2025). *Science's big problem is a loss of influence, not a loss of trust*, Nature. *https://www.nature.com/articles/d41586-025-01068-1*

Liens consultés le 22 septembre 2025.

Annexe
Comité éditorial et personnes consultées

Annexe

Membres du comité éditorial

Julie Dirwimmer, Fonds de recherche du Québec (coordination)

Philippe Bettez-Quessy, Secrétariat du Conseil du Trésor du Québec

Martin Boucher, ministère du Conseil exécutif du Québec

Marie-Ève Carignan, Université de Sherbrooke

Dave Castegan, ministère de la Sécurité publique du Québec

Christian Cossette, ministère de la Cybersécurité et du Numérique du Québec

Jean Dubé, Association des directeurs généraux des municipalités du Québec

Philippe Dubois, École nationale d'administration publique

Steve Jacob, Université Laval

Pascal Lapointe, Agence Science-Presse

Kathia Légaré, Commission d'éthique en science et en technologie du Québec

Émilie Michaud, Fonds de recherche du Québec

David Morin, Université de Sherbrooke

Stéphane Paquin, École nationale d'administration publique

Véronique Sauriol, Fonds de recherche du Québec

Samuel Tanner, Université de Montréal

Thierry Warin, HEC Montréal

Personnes consultées

Guillaume Bergeron, ministère de la Cybersécurité et du Numérique du Québec

Cassandra Carrier, secrétariat du Conseil du Trésor du Québec

François Ducharme, TACT Conseil

Vanessa Fournier, ministère de la Sécurité publique du Québec

Antoine Gagnon, Assemblée nationale du Québec

Thierry Giasson, Université Laval

Anick Laplante, Assemblée nationale du Québec

Monika Smaz, ministère de la Cybersécurité et du Numérique du Québec

Martin Soucy, ministère de la Cybersécurité et du Numérique du Québec

Nicolas Vermeys, Université de Montréal