CRYPTO.QUÉBEC

ON VOUS TROMPE

Comprendre la **mésinformation**,
les **mensonges** et la **manipulation** en ligne

TRÉCARRÉ

INTRODUCTION

Lorsque notre éditrice nous a approchés pour écrire un deuxième livre, nous nous sommes tout d'abord demandé si nous étions les bonnes personnes pour traiter l'important sujet de la désinformation en ligne.

Notre petit organisme bénévole, quelques années après la publication de notre premier livre, traversait une période de grands changements. Il accueillait des bénévoles tout frais, se voyait offrir de nouveaux mandats, affrontait des enjeux grandissants… dans le contexte inégalé d'une pandémie, d'une tentative de coup d'État aux États-Unis, d'une propension importante au télétravail, d'un sentiment d'isolement et de débats incessants sur les réseaux sociaux à propos de tout : vaccins, élections, passeport vaccinal, etc.

La mission de Crypto.Québec, qui embrassait déjà la surveillance, la protection de la vie privée et les enjeux géopolitiques liés au piratage informatique, a été appelée à s'étendre officiellement à la littératie numérique de nos concitoyens, y compris au

discernement du vrai et du faux dans les informations en ligne. Cet enjeu est devenu de plus en plus complexe au gré des progrès en intelligence artificielle (IA) et dans les technologies de reconnaissance faciale, de l'explosion de *Big Data* (des mégadonnées) et des usines à contenus qui ont désormais maîtrisé l'art d'alimenter des centaines de pages web afin de créer des écosystèmes entiers de fausses nouvelles, d'attaques par rançongiciels… sans compter les autres arnaques qui pullulent sur les réseaux sociaux ou dans nos boîtes de courriel et qui se multiplient à une vitesse effarante. Un vrai fléau du Web 2.0.

UN HOMME POLITIQUE, UNE MARKETEUSE, UNE JOURNALISTE, UN MÉDECIN, UN SOCIOLOGUE ET UN ÉCONOMISTE ENTRENT DANS UN BAR…

Notre nouvelle équipe d'autrices et d'auteurs a vite fait de constater que nous avions tous des parcours atypiques, que nous étions tous des « ex-quelque chose » qui avions choisi de nous intéresser à la cybersécurité afin d'en devenir des professionnels. Drôlement, ces regards variés nous ont probablement permis de nous intéresser d'une façon plus humaine à la question de la manipulation sur Internet. Car il est impossible de dissocier les nombreuses arnaques, fausses nouvelles et autres malicieux périls qui nous guettent en ligne de leurs conséquences bien réelles sur les humains qui cliquent dessus ou y croient. Aujourd'hui, 95 % des attaques informatiques dépendent, à un moment ou à un autre, d'une opération d'ingénierie sociale, soit le piratage du cerveau humain, sujet que nous avons

exploré dans *On vous voit*. La désinformation fonctionne selon les mêmes principes.

Pour Crypto.Québec, ce deuxième livre est donc une tentative, d'humains à humains, de nous protéger et de limiter les contrecoups de ces malicieuses tentatives de tromperie sur notre société.

L'ÉQUIPE

Diplômée en communication-marketing, Catherine s'entête à ne pas travailler dans son domaine d'études, en choisissant plutôt de réaliser des projets d'affaires, d'enseigner au collégial ou de faire des analyses de sensibilisation. Passionnée et enthousiaste, elle a trouvé dans la cybersécurité un domaine qui lui permet de vivre sa passion pour la technologie, la communication et la pédagogie.

Luc, notre geek humaniste et l'un des fondateurs de Crypto.Québec, a eu plusieurs vies. Il a notamment participé à la fondation du parti Option nationale, et sa carrière suit le même fil conducteur : le service public, le renforcement du bien commun, la protection de la vie privée et la défense de la démocratie. Expert en gouvernance de la sécurité de l'information de jour et président-cofondateur de Crypto.Québec de soir.

Fanny est journaliste spécialisée en technologie. Elle s'intéresse aux enjeux sociaux et politiques du numérique, en particulier à la surveillance de masse et à la protection de la vie privée, à la cybersécurité, à la propagande computationnelle et aux luttes de pouvoir dans le cyberespace.

Médecin de formation, Sam a troqué son stéthoscope contre le clavier. Comme journaliste et programmeur passionné par la cybersécurité, il écrit aujourd'hui des textes et du code. Il s'intéresse particulièrement aux enjeux politiques et sociaux des algorithmes.

Ancien étudiant en actuariat, passionné d'informatique et de nouvelles technologies, Samuel, lui, s'intéresse aux enjeux de cybersécurité et d'intégrité des données depuis de nombreuses années. Plus récemment, il s'est tourné vers tout ce qui touche aux chaînes de blocs ainsi qu'au développement durable.

Enfin, Jimmy, sociologue de formation, a orienté sa carrière vers la sécurité électronique. Il s'intéresse au déploiement des technologies de surveillance, à leurs contre-mesures et à leurs conséquences, tant négatives que positives, sur la société, l'économie et le politique. Il vit de cinq à dix ans dans le futur quant aux tendances technologiques et aux enjeux sociaux émergents.

Ensemble, les auteurs de cet ouvrage se sont questionnés sur le phénomène des tromperies en ligne. Leur démarche s'étend de la désinformation aux arnaques amoureuses en passant par les grands débats sur le *Big Data*, la radicalisation en ligne et l'hypertrucage (*deepfake*).

CRYPTOGRAPHIE, PAS CRYPTOMONNAIE !

Avec un nom comme Crypto.Québec et connaissant l'engouement d'une partie de la population pour les

cryptomonnaies, il est difficile pour nous de ne pas aborder la question, ne serait-ce qu'en introduction ; nous recevons à ce sujet des dizaines de messages tous les jours, au grand dam de Luc.

Le nom de notre organisme vient du mot « cryptographie », défini par Wikipédia comme « l'une des disciplines de la cryptologie, s'attachant à protéger des messages (pour assurer leurs confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou de clés ». En parallèle, les cryptomonnaies – le bitcoin, le dogecoin et l'ethereum étant parmi les plus célèbres – donnent lieu à des systèmes monétaires privés et décentralisés, et donc dérégulés, pour le meilleur et pour le pire. Leur popularisation récente, soutenue par leur adhésion aux grandes plateformes d'échange telles que WealthSimple ou RobinHood, aux États-Unis, a eu une série de conséquences sur l'écosystème de la planète[1] et du Web.

Quel est le lien exact entre cybersécurité et cryptomonnaie ? Eh bien l'un des grands dilemmes auquel fait face un criminel en ligne est le déplacement de grandes quantités d'argent de façon anonyme. Et l'un des grands avantages de la cryptomonnaie est qu'elle permet de déplacer de grandes quantités d'argent à l'abri des regards indiscrets ! D'ailleurs, au moment d'écrire ces lignes, on apprend l'un des plus grands vols de cryptomonnaie à ce

1. En dehors des enjeux de cybersécurité et de leurs influences dans les manœuvres frauduleuses et d'autres tromperies en ligne, notons que la popularité des cryptomonnaies comporte de grands enjeux environnementaux.

jour, soit l'équivalent de 600 millions de dollars ethereum[2].

Grâce à la cryptomonnaie, un individu (ou une entreprise) peut s'attaquer aux systèmes informatiques d'une organisation, par exemple d'un hôpital[3], puis exiger et recevoir une rançon qu'il pourra ensuite blanchir de façon relativement anonyme, à moins d'être impliqué dans un scandale aviaire qui fera lever des soupçons sur sa grande et soudaine richesse[4].

L'ampleur du problème des rançongiciels est rendue si grande que nous avons constaté récemment l'arrivée de « rançongiciels en tant que service » (*Ransomware as a service*[5]). Il s'agit d'organismes spécialisés qu'on peut mandater pour compromettre une autre entreprise. Le service est si rentable que ce genre d'entreprise va même jusqu'à offrir à sa clientèle un service de clavardage pour accompagner les victimes dans le paiement de leur rançon, les guidant, étape par étape, dans la création d'un compte permettant de faire un transfert de bitcoins afin de récupérer les données compromises.

Les bitcoins facilitent donc les attaques en ligne et, du coup, nous rendent tous un peu plus vulnérables. Selon Yonatan Striem-Amit, cofondateur de

---

2. https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain

3. https://ici.radio-canada.ca/nouvelle/1745268/attaque-informatique-hopitaux-canada-etats-unis-quebec-virus-rancon

4. https://www.ledevoir.com/societe/658485/voyage-des-influenceurs-l-organisateur-tente-de-s-expliquer

5. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas

la société de cybersécurité Cybereason : « C'est vraiment un outil très puissant entre les mains des criminels pour blanchir de l'argent, pour transférer des devises d'un État à un autre d'une manière qui est en un sens introuvable et définitivement incontrôlable[6]. »

Bref, l'équipe de Crypto.Québec ne vous aidera pas à investir ni à mousser votre nouvelle devise décentralisée, mais nous aborderons au chapitre 6 les arnaques les plus courantes en ligne. Celles-ci visent à exploiter la curiosité des gens souhaitant s'enrichir rapidement en plaçant leurs économies dans les monnaies qui font fureur sur Twitter.

VOUS PROTÉGER : VOUS, VOS PROCHES ET… NOTRE DÉMOCRATIE

Il est difficile de bien calculer les conséquences réelles de la désinformation, des théories du complot et d'autres arnaques en ligne sur notre société.

Selon les *Proceedings of the National Academy of Sciences of the United States of America*, une revue scientifique multidisciplinaire dont les articles sont révisés par les pairs : « Depuis l'élection présidentielle américaine de 2016, la propagation délibérée de la désinformation en ligne, et sur les réseaux sociaux en particulier, a suscité une inquiétude extraordinaire, en grande partie en raison de ses effets potentiels sur l'opinion

6. https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks)

publique, la polarisation politique et, finalement, la prise de décision démocratique[7]. »

Étant donné la complexité de la question, il faudra élaborer des modèles afin de pouvoir observer de façon rigoureuse les conséquences de la désinformation en ligne.

Selon Statistique Canada, on sait qu'« au cours des premiers mois de cette crise sanitaire, 96 % des Canadiens ayant utilisé Internet pour s'informer ont vu des informations sur la COVID-19 qu'ils ont soupçonnées d'être trompeuses, fausses ou inexactes. Parmi eux, le quart (25 %) a vu des informations suspectes plusieurs fois par jour, 14 %, une fois par jour, et 29 %, au moins une fois par semaine. Un peu moins du tiers des Canadiens (28 %) ont indiqué avoir rarement vu de fausses informations et 4 % ont répondu ne jamais en avoir vu ».

De plus, près de deux Canadiens sur cinq (40 %) ont rapporté avoir déjà cru que des informations liées à la COVID-19 étaient vraies pour ensuite réaliser que ce n'était pas le cas[8]. Également, selon un sondage réalisé par Léger Marketing, « deux Canadiens sur cinq (40 pour cent) considèrent qu'il est "certainement" ou "probablement" vrai » que « certains événements importants sont le résultat de l'activité d'un petit groupe qui manipule secrètement les événements mondiaux[9] ». C'est donc 40 %

7. https://www.pnas.org/doi/10.1073/pnas.1912443118

8. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00003-fra.htm

9. https://globalnews.ca/news/8329274/canadians-conspiracy-theories-trust-institutions-poll/

d'entre nous qui croient dans une certaine mesure aux conspirations telles que QAnon (voir plus loin).

Alors que la présence de QAnon se fait sentir un peu partout dans le monde, le Canada abriterait l'une des plus grandes communautés d'adeptes de ce culte[10]. Et comme ces théories conspirationnistes tendent à être politisées, il est logique de penser qu'elles influent sur nos décisions politiques, particulièrement en période d'élection. Nous examinerons les conséquences du culte de QAnon plus en détail au chapitre 2, son effet sur la fenêtre d'Overton (au chapitre 1) et les enjeux de société qui en découlent.

Nous savons également qu'en 2021 la fraude en ligne a causé des pertes de 275 M$ au Canada[11]. Puisqu'une grande partie des fraudes ne sont pas déclarées, on peut s'imaginer qu'il ne s'agit là que de la pointe de l'iceberg. Ces fraudes ont un effet sur notre économie et, à plus petite échelle, sur les victimes qui en souffrent, certaines fraudes étant de nature particulièrement intime (voir chapitre 5). Au Québec, au cours des dernières années, ce sont nos institutions qui ont été la cible d'attaques informatiques : nos hôpitaux, nos sociétés de transport et même nos municipalités. Au-delà des pertes financières, nos données personnelles et nos systèmes de logistique sont menacés : la possibilité d'une attaque à grande échelle sur notre réseau électrique, par

10. https://montreal.ctvnews.ca/how-canada-became-one-of-the-world-s-biggest-hubs-for-qanon-conspiracy-theories-1.5172097

11. https://ici.radio-canada.ca/nouvelle/1870131/arnaque-investissement-vol-finance-banque-fraude-canada

exemple, est un enjeu avec lequel il faut composer, compte tenu des conséquences désastreuses qui en découleraient[12].

Toutefois, ce qui se passe en ce moment sur le Web n'a pas simplement un effet sur nos fils de nouvelles virtuelles : comme bien des gens, vous avez peut-être perdu un proche, des amis, des collègues ou de la famille à cause des théories du complot ou à la suite de débats ultrapolarisés sur les réseaux sociaux. La polarisation, un phénomène que nous aborderons au chapitre 1, influe sur nos débats démocratiques : comment discuter, en tant qu'expert en cybersécurité, des enjeux de vie privée tels que le contrôle de l'accès à des preuves vaccinales si notre opposition à cette mesure nous classe automatiquement parmi les conspirationnistes ? C'est comme s'il n'y avait plus de position nuancée entre l'acceptation de toutes les mesures et le fait de s'y opposer formellement (pour des raisons parfois douteuses, parfois légitimes).

L'ensemble de ces éléments influe finalement sur notre tissu social qui semble en avoir pris un coup ces dernières années[13] : isolement social, écart de richesse, écoanxiété, algorithmes favorisant la discorde, baisse de confiance, augmentation des méfaits en ligne, etc. Notre climat social actuel encourage la méfiance et la colère envers nos institutions ainsi qu'un individualisme qui s'oppose fermement au bien collectif. Cet

12. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector

13. https://www.theatlantic.com/politics/archive/2022/03/antisocial-behavior-crime-violence-increase-pandemic/627076/

isolement nous rend vulnérables à l'endoctrinement, sujet que nous aborderons dans les chapitres sur la radicalisation en ligne. La colère et la méfiance, elles, nous rendent fragiles à la propagande autoritaire[14]. La peur est un outil politique efficace dans la mise en place de mesures liberticides, antidémocratiques et divisives, particulièrement envers les minorités et les membres vulnérables de nos collectivités.

Nous perdrions également confiance en nos institutions : 49 % des Canadiens croient que les journalistes tentent de les flouer volontairement[15]. Que ce soit parce qu'il y a un manque de transparence entre nos décideurs, nos médias et les algorithmes qui nous proposent des contenus ou encore parce que la flamme de la méfiance est attisée par des agents mal intentionnés qui souhaitent magnifier nos craintes pour mieux les exploiter politiquement, il est de plus en plus évident que nous devons, en tant que citoyens du Web, veiller à bien nous informer, à garder un œil sur nos médias afin d'en préserver l'intégrité et à protéger notre démocratie en restant vigilant devant les nombreuses tromperies que nous croiserons en ligne.

Dans les démocraties, les médias sont généralement considérés comme un « quatrième pouvoir », c'est-à-dire le contrepoids aux branches de l'État ayant les pouvoirs législatif, exécutif et judiciaire. Ce contrepoids permet à la population de tenir le gouvernement redevable de ses actions tout en prenant

---

14. https://theconversation.com/the-politics-of-fear-how-fear-goes-tribal-allowing-us-to-be-manipulated-109626

15. https://www.cbc.ca/news/editorsblog/editor-blog-trust-1.5936535

des décisions éclairées. Aujourd'hui, le quatrième pouvoir est en pleine transformation : les journalistes sont désormais en concurrence pour des clics sur les réseaux sociaux, les informations recueillies doivent être publiées à une vitesse fulgurante, ce qui rend très difficile la vérification ; les médias de divertissement se présentent telles des salles d'information, à la manière de Fox News ; les risques inhérents au métier journalistique, dont les assassinats, les incidents d'espionnage, le harcèlement en ligne et la violence générale, plus particulièrement à l'égard des femmes selon un rapport publié par l'UNESCO, se multiplient[16].

LA LITTÉRATIE NUMÉRIQUE POUR TOUS

Les membres de Crypto.Québec croient fermement que l'une des solutions à la plupart des problèmes que nous venons de nommer est le rehaussement de la littératie numérique de nos concitoyens. En vous sensibilisant aux enjeux numériques et à l'importance d'être vigilant en ligne, vous saurez mieux repérer les tentatives de désinformation, de fraude et d'usurpation et vous protéger, vous et vos proches, contre elles, vous pourrez former des opinions ancrées dans la réalité et les faits, et vous serez outillé pour faire face à un paysage médiatique de plus en plus complexe, décentralisé et dérégulé. N'oubliez pas qu'Internet, c'est le *Far West*!

16. https://en.unesco.org/courier/2021-4/journalism-dangerous-profession

Alors que notre premier livre abordait principalement la protection de vos données privées en ligne, le présent ouvrage se veut un cours d'autodéfense contre les menaces auxquelles nous sommes exposés sur le Web, tant à l'échelle individuelle (recevoir un courriel d'hameçonnage) qu'à l'échelle de la société (se faire inonder de désinformation et de propagande). En ligne, on vous trompe. Apprenons à contrecarrer les tentatives des agents malicieux.

1. MÉSINFORMATION *VERSUS* DÉSINFORMATION

« Prochaine station : Berri-UQAM ! »

Jessica est sous le choc : elle vient de lire une publication sur Facebook partagée par son cousin au sujet des risques, cachés par les médias, d'un médicament en vente libre bien connu qu'elle utilise couramment. Outrée d'apprendre qu'elle se serait exposée à toutes sortes de dangers, elle republie rapidement un graphique contenu dans le statut initial, jurant au passage de jeter à la poubelle tous les produits de cette marque dès son retour à la maison. Quel scandale !

Quelques « J'aime » plus tard, reçus notamment de son cousin et d'une de ses copines d'école, Jessica arrive à sa destination. Elle glisse son téléphone dans sa poche, sort du métro et entre dans son bureau où elle s'empresse d'informer un collègue de sa lecture inquiétante. Le sourire aux lèvres, elle se sent un peu comme une héroïne des temps modernes : grâce à son partage matinal, elle a peut-être sauvé des individus de cancers ou d'autres maux horribles ! C'est

fou comme on ne peut plus faire confiance aux médias traditionnels ! Cette nouvelle aurait pourtant dû faire la une de tous les journaux de la province…

Une semaine plus tôt, une firme de relations publiques aux pratiques douteuses s'est demandé comment convaincre des consommateurs d'opter pour un nouveau produit « naturel », non homologué par Santé Canada, aux dépens d'un produit bien établi depuis des années. En utilisant un réseau de sites qui lui appartiennent, la firme a élaboré une campagne de désinformation dans le but de faire douter d'un médicament qui n'a pourtant jamais fait l'objet de controverses médicales réelles.

Une équipe de créateurs de contenu s'est mise rapidement à l'œuvre : articles de blogue, faux reportages, analyses manipulées d'études non révisées par les pairs, images faciles à repartager et octroi de contrats alléchants à des « gourous » de la santé sur Instagram qui annonceront un lien « secret et jusqu'ici caché par les médias » entre le médicament et des risques de cancer foudroyant. La machine à fausses nouvelles s'est mise en branle[1]. La campagne se propage tel un virus sur les réseaux sociaux, elle est même traduite dans plusieurs langues. Des milliers de clics, partages et « J'aime » plus tard, le doute est semé dans l'esprit de nombreux consommateurs partout dans le monde. Il ne reste alors à l'agence de relations publiques plus qu'à viser, à l'aide de messages ciblés, tous ceux et celles qui ont cru aux publications mensongères afin

1. https://arstechnica.com/tech-policy/2021/10/disinformation-guru-hacker-x-names-his-employer-naturalnews-com/

de leur proposer une solution « holistique ». L'achat du remède « miracle » sera proposé sur un site partenaire faisant partie du réseau de l'agence, qui récoltera une généreuse commission sur les ventes de la nouvelle vitamine fabriquée en passant à l'étranger, où aucun cadre réglementaire n'a démontré son efficacité… ni sa sûreté !

C'EST L'INTENTION QUI COMPTE

Lorsqu'on tente de distinguer mésinformation et désinformation, ce qui sépare ces deux actions, c'est l'intention.

Dans le cas de Jessica, le partage s'est fait avec les meilleures intentions : le désir de protéger ses proches d'un danger auquel elle a été sensibilisée par son cousin, en qui elle a confiance et qui a été le premier à publier l'information. On parle donc ici de *mésinformation.* La nouvelle est alarmante et provoque une réaction émotionnelle. Dans le métro, en route vers le travail, Jessica n'a pas les outils, le temps ni le réflexe de vérifier cette nouvelle si ce n'est de noter qu'aucun média d'envergure ne semble en parler. Bien entendu, ils n'en parlent pas parce qu'il n'y a rien de concret à discuter : aucune étude n'a révélé de lien entre le produit et des risques accrus de cancer. La « nouvelle » est le produit d'une campagne de désinformation coordonnée par une agence de relations publiques malicieuse.

Cette agence qui a créé, publié et exploité, en toute connaissance de cause, l'information mensongère est coupable de *désinformation.* Elle a communiqué chaque fausse information intentionnellement, dans le but de

tromper. Parfois, la tromperie est construite à des fins commerciales, parfois elle soulève de plus grands enjeux d'ordre politique. Souvent, il s'agit un peu des deux.

Il reste que… ça ne s'invente pas, tout ça ! Récemment, un lanceur d'alerte a dénoncé une situation très similaire au sujet d'un populaire site de désinformation spécialisé en « nouvelles » de santé naturelle. L'élément déterminant pour ce pirate dans sa décision de dénoncer son ex-employeur ? Une discussion avec son père âgé qui avait choisi de refuser le vaccin contre la COVID-19. Convaincu par les idées conspirationnistes autour du vaccin, le vieux monsieur n'en démordait pas, malgré l'imploration de son fils, qui finit par lui avouer avoir écrit tous les textes auxquels il s'accrochait.

À un moment ou un autre, on a tous été victimes d'un clic trop rapide, fait dans l'émotion. L'important, c'est d'acquérir de bonnes habitudes avant de cliquer, de partager et surtout de croire l'information lue sur le Web.

Mésinformation
Partage d'information qui n'est pas factuelle sans le savoir. La personne ou l'organisme qui fait de la mésinformation est de bonne foi.

Désinformation
Création et partage d'information fausse ou manipulée. La personne ou l'organisation agit en toute connaissance de cause.