UNIVERSITÉ DU QUÉBEC À MONTRÉAL

STRATÉGIE ET TACTIQUE À L'ÈRE DES MÉGADONNÉES : ANALYSE CRITIQUE DU DISCOURS DE CRYPTO.QUÉBEC

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN COMMUNICATION

PAR
JIMMY PROULX-ROY

OCTOBRE 2019

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce mémoire se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév.07-2011). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

« Nous avons une responsabilité : protéger vos données.
Si nous n'y parvenons pas, nous ne les méritons pas [traduction libre] ».

Mark Zuckerberg, p.-d. g. de Facebook, 2018

REMERCIEMENTS

Après plusieurs mois de recherche et de rédaction, je tiens à témoigner mes sincères remerciements à toutes les personnes qui ont contribué de près ou de loin au bon déroulement de mon mémoire de maîtrise. Tout d'abord, mon directeur de recherche, André Mondoux, pour sa disponibilité, son efficacité, ses précieux conseils et sa réelle passion qui ont contribué à alimenter ma réflexion et qui m'ont surtout aidé à persévérer tout au long du processus de recherche. Également, je tiens à remercier ma conjointe pour son support et son accompagnement durant toutes ces années. Je n'aurais pu réussir sans son aide des plus précieuses dans toutes les sphères de ma vie. Aussi, je remercie ma famille, ma belle-famille et mes amis pour leur immense soutien. Certes, j'ai eu le plaisir de travailler sur un sujet qui me passionne, les mégadonnées. Et dire que les données de ce mémoire seront hébergées en ligne comme une goutte d'eau dans l'océan numérique. Merci à tous ceux et celles qui poursuivront les recherches dans ce domaine.

TABLE DES MATIÈRES

LISTE DES FIGURES vii

LISTE DES TABLEAUX viii

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES ix

RÉSUMÉ x

INTRODUCTION 1

CHAPITRE 1
PROBLÉMATIQUE 5

1.1. Mise en contexte 5

1.2. Revue de la littérature 15

1.2.1. Des solutions individuelles pour protéger la vie privée 15

1.2.2. Des solutions techniques pour protéger la vie privée 18

1.2.3. Question générale de recherche 20

CHAPITRE 2
CADRE THÉORIQUE 23

2.1. Les modes de reproduction de la société 23

2.2. Gouvernementalité et rapports de pouvoir 31

2.3. Stratégie et tactique 35

2.4. Questions de recherche 42

2.5. Pertinence et originalité 44

2.5.1. Pertinence sociale 44

2.5.2. Pertinence scientifique 45

CHAPITRE 3
MÉTHODOLOGIE QUALITATIVE 46
3.1. Choix de l'objet de recherche 46
3.1.1. Crypto.Québec 46
3.1.2. Sélection du corpus discursif 48
3.2. Analyse critique du discours 49
3.2.1. Les principes fondamentaux de l'ACD 49
3.2.2. L'analyse de discours idéologique 52
3.3. Analyse du discours de Crypto.Québec 53
3.3.1. Grille d'analyse et encodage 53
3.3.2. Personnalisation et utilisation d'un document inspiré du logiciel TAMS Analyser 56
CHAPITRE 4
RÉSULTATS 60
4.1. Changer les habitudes de la population 60
4.1.1. Des conseils d'experts 62
4.1.2. Des services pour se rapprocher de la communauté 64
4.1.3. Les défis 66
4.2. Influencer les décisions de demain 69
4.2.1. Réfléchir à de nouveaux modèles d'affaires 70
4.2.2. Les défis 71
4.2.2.1. Peu de débats au Québec selon l'organisme 71
4.2.2.2. Des ressources limitées pour Crypto.Québec 73
4.3. De l'individu à la société 74
4.3.1. De la prise de conscience individuelle à des changements collectifs 74
4.3.2. Des *hackers* à l'enseignement universitaire 76

CHAPITRE 5
INTERPRÉTATION DES RÉSULTATS 78
5.1. Le circuit marchand des mégadonnées au cœur des discussions 78
5.2. Les GAFAM et le mode de reproduction décisionnel-opérationnel 81
5.3. Les rapports de pouvoir et les points de fuite : des conseils et des services comme tactiques de détournement 83
5.3.1. Les protagonistes 83
5.3.2. Les rapports de pouvoir et les points de fuite 86
5.3.3. Des conseils et des services comme tactiques de détournement 89
5.4. Stratégie et Crypto.Québec 94
CONCLUSION 101
ANNEXE 1 TABLEAU DE BORD DE GOOGLE ANALYTICS 110
ANNEXE 2 CORPUS DES DOCUMENTS SÉLECTIONNÉS 111
ANNEXE 3 PAGE WEB D'UNE ÉMISSION DE *LES CHIENS DE GARDE* 118
ANNEXE 4 GUIDE DE DÉTOX EN 8 JOURS 119
BIBLIOGRAPHIE 120

LISTE DES FIGURES

Figure Page

1.1. Module du bouton « J'aime » de Facebook..... 19

A.1. Tableau de bord de Google Analytics..... 110

A.3. Page Web d'une émission de *Les chiens de garde*..... 118

A.4. Guide de détox en 8 jours..... 119

LISTE DES TABLEAUX

Tableau		Page
3.1.	Grille d'analyse	55
3.2.	Exemple de collecte de données	58
A.2.	Corpus des documents sélectionnés	111

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ACD	Analyse critique du discours
GAFAM	Google, Amazon, Facebook, Apple et Microsoft
OSBL	Organisme sans but lucratif
NSA	Agence nationale de la sécurité américaine
NTIC	Nouvelles technologies de l'information et de la communication

RÉSUMÉ

Le monde produit des données à un rythme inquiétant. Les plateformes en ligne des grandes compagnies technologiques, notamment les GAFAM, sont conçues pour soutirer un maximum d'informations sur les usagers, sans même être remises en question. Les mégadonnées permettent d'en savoir beaucoup sur les usagers et peuvent représenter des risques d'identification et de surveillance pouvant compromettre leur vie privée. Dans un tel contexte, l'objectif de cette recherche est d'explorer la possibilité pour un organisme de sensibilisation de contourner (ou détourner) les usages prescrits par les GAFAM avec la théorie de Michel De Certeau (1990). Le cadrage théorique est notamment inspiré des concepts de cet auteur qui sont la stratégie et la tactique, du mode de reproduction décisionnel-opérationnel de Michel Freitag et des rapports de pouvoir chez Michel Foucault. Pour y parvenir, l'étude propose une analyse critique du discours de Crypto.Québec, un organisme sans but lucratif qui a pour mission de vulgariser les enjeux de sécurité informatique et de vie privée. Ce type de méthode qualitative permet un regard critique sur la domination exercée par les entreprises privées, en plus d'explorer les différentes tactiques utilisées par l'organisme. Les données recueillies proviennent essentiellement d'émissions en baladodiffusion et d'interventions médiatiques créées par ou avec la participation de l'organisme sur une période d'un an. L'analyse met en lumière les tactiques de détournement (conseils d'experts, offre de services) utilisées par Crypto.Québec pour faire face aux GAFAM, mais aussi pour mener de manière stratégique le public de l'organisme vers un lieu propre qui rejoint sa mission. Les résultats permettent de conclure qu'il est possible pour l'organisme d'encourager les usagers à contourner les GAFAM par l'entremise de tactiques de détournement. Cependant, ces pratiques de détournement se doivent d'être institutionnalisées si elles veulent engendrer un changement significatif, permanent et durable en matière de protection de la vie privée en ligne. Enfin, cette recherche justifie la pertinence pour une prise de conscience sur les mégadonnées et fournit des connaissances à tout lecteur-usager soucieux de sa présence numérique.

Mots-clés : tactique, stratégie, mégadonnées, vie privée, GAFAM, médias socionumériques, analyse critique du discours.

INTRODUCTION

Lorsque Sun Tzu, général chinois du IVe siècle avant J.-C., s'interrogeait dans *L'Art de la guerre*, il disait : « Qui connaît l'autre et se connaît, en cent combats ne sera point défait ; qui ne connaît l'autre mais se connaît, sera vainqueur une fois sur deux ; qui ne connaît pas plus l'autre qu'il ne se connaît sera toujours défait » (Tzu, ~400 av. J.-C. / 2015 : 61). L'armée a été l'un des premiers types d'organisations à se doter de « stratégies » pour défaire un adversaire, nécessitant de la ruse, de l'audace et de la créativité. Étymologiquement parlant, la stratégie est empruntée au terme grec *strategia* qui signifie « commandement d'une armée » (CNRTL, s. d.). Le stratège prépare un plan généralement fondé sur un objectif précis qui permet « d'anticiper tous les facteurs qui pourraient avoir un impact sur cet objectif visé » (Gambier, 2009 : 64). Tout comme un général qui doit déplacer d'une certaine manière ses combattants sur un champ de bataille, un joueur d'échecs est également amené à disposer ses pièces d'une certaine façon sur un échiquier. Xavier Tartakover, l'un des célèbres joueurs d'échecs du 20^{e} siècle, avait une explication pour décrire cette dynamique entre la stratégie et la tactique : « La tactique consiste à savoir ce qu'il faut faire quand il y a quelque chose à faire. La stratégie consiste à savoir ce qu'il faut faire quand il n'y a rien à faire[1] » (Hooper et Whyld, 1987 : 346). La tactique, quant à elle, provient du terme *taktikós* qui signifie « l'art de ranger ou de faire manœuvrer des troupes » (CNRTL, s. d.). La tactique peut consister à réaliser « des actions coordonnées » (*op. cit.*, Gambier, 2009 : 64).

[1] Traduction libre

Les stratégies et les tactiques sont des concepts riches et intrigants, étudiés de nos jours dans plusieurs autres domaines (politique, marketing, sport, etc.). Comme nous le verrons tout au long de notre mémoire, elles constituent un élément clé de notre thématique de recherche qui se situe dans l'étude des nouvelles technologies de l'information et de la communication (NTIC), et plus particulièrement dans l'usage des plateformes en ligne à l'ère des mégadonnées.

De nos jours, des plateformes numériques continuent à être développées sans nécessairement dévoiler leurs objectifs ou leurs principes fondamentaux. Nous avons des usagers (soldats) qui manipulent les fonctionnalités de ces plateformes créées par des entreprises privées (armée), mais également certains usagers qui cherchent à utiliser ces plateformes d'une manière différente (un soldat qui se révolte, un déserteur, etc.). Ces usagers sont soucieux, angoissés, dubitatifs et s'éloignent de la ligne de bataille à la recherche d'un emplacement qui les rendrait plus confortables. Qui sont ces usagers ? Comment et pourquoi le font-ils ? Quelles sont leurs intentions ? Avec l'arrivée d'Internet, la quantité d'informations disponibles peut être l'une de leurs principales motivations. Les usagers circulent au quotidien dans un univers où leurs interactions deviennent de l'information pouvant être captée et mesurée. Pour revenir au champ de bataille, les renseignements que peut soutirer une armée de son adversaire ont une valeur considérable et peuvent la conduire vers une victoire : connaître sa position, son comportement, ses méthodes, ses forces, ses faiblesses, etc. Actuellement, Internet offre la possibilité aux gouvernements et aux entreprises privées de cumuler des données sur les usagers : leur position géographique, leur comportement en ligne, leurs intérêts, le temps perdu à flâner, etc. Ainsi, notre préoccupation se situe au niveau de l'information disponible à propos des usagers. À qui sert-elle vraiment ? Dans quel but ? Si les usagers ne veulent pas fournir autant d'information aux plateformes en ligne tout en continuant à les utiliser, quels sont les moyens à leur disposition ? Nous souhaitons y voir plus clair dans cet univers de données et c'est pourquoi nous nous penchons sur la relation entre la

tactique, la stratégie et les usages des NTIC. Nous pensons qu'il s'avère intéressant d'étudier ce qui fait que les usagers se sentent inconfortables avec l'utilisation de leurs données par les entreprises qui les dirigent.

Pour mener à bien ce mémoire, notre étude sera organisée en cinq chapitres. Le premier porte sur la problématique de notre recherche. Nous y situons d'abord le contexte qui entoure notre thématique de recherche, notamment l'ère des mégadonnées. Nous faisons ensuite un survol de la littérature sur les enjeux liés à la collecte de données et sur les NTIC qui laissent envisager des formes de surveillance et d'identification.

Notre deuxième chapitre présente notre cadre théorique. Nous y avançons les concepts clés de la tactique et de la stratégie du philosophe français Michel de Certeau, en plus d'aborder les théories des chercheurs Michel Freitag et Michel Foucault, un cadre de référence nécessaire pour mieux saisir le monde numérique dans lequel nous vivons. Nous y abordons également les questions, les objectifs et la pertinence de notre recherche.

Le troisième chapitre porte sur le volet méthodologique. Nous introduisons l'objet de recherche, l'organisme Crypto.Québec et les raisons de son choix. Nous y spécifions le corpus des données collectées ainsi que la méthode qualitative choisie pour permettre l'analyse des résultats, soit l'analyse critique du discours (ACD). En outre, nous abordons les principes fondamentaux de l'ACD en plus d'aborder une version de celle-ci, l'analyse de discours idéologique du chercheur Teun A. Van Dijk. Nous précisons enfin la grille d'analyse employée et un document inspiré du logiciel TAMS Analyser servant à la collecte de données.

Le quatrième chapitre rassemble la présentation des résultats, où nous rapportons de façon descriptive les différents résultats obtenus. Nous rassemblons sous différentes

thématiques ce qui a été dégagé du discours de Crypto.Québec, notamment les pratiques de sensibilisation de l'organisme et les défis qui les entourent.

Le cinquième et dernier chapitre est consacré à l'analyse des résultats, une interprétation sommaire de nos résultats avec les thèmes abordés dans la problématique et le cadre théorique afin de nous aider à répondre à nos questions de recherche.

CHAPITRE 1

PROBLÉMATIQUE

Dans ce premier chapitre, nous abordons l'écart entre ce que nous savons, ce qui est déjà connu dans la littérature et ce que nous aimerions savoir. En d'autres termes, il s'agit d'une organisation d'éléments théoriques « de manière à faire émerger une figure, une constellation, nouvelle ou connue, correspondant ici à notre problème de recherche » (Mongeau, 2008 : 52).

1.1. Mise en contexte

Les nouvelles technologies de l'information et de la communication (NTIC), c'est-à-dire « les techniques, outils et méthodes utilisés pour faciliter les communications » (Melody, 2006) ont évolué rapidement dans les quatre dernières décennies. Depuis les années 80, le développement des infrastructures informatiques et l'amélioration continue des réseaux mobiles ont permis d'augmenter la portée d'accès à Internet, préparant le terrain pour des appareils technologiques incontournables pour communiquer (*Ibid.*, 2006). Au cours des années 1990 et 2000, nous avons vu des technologies tels la télévision, le téléphone et le télécopieur converger vers de nouvelles technologies liées à Internet. La progression est telle que nous avons affaire à une « explosion du nombre de nouveaux objets techniques de communication mis en marché [...] et le foisonnement des applications logicielles qui démultiplient leurs utilisations possibles » (Proulx, 2002 : 180). Par exemple, le nombre de téléphones

mobiles existants dépasse depuis quelques années celui de la population mondiale (Boren, 2014). Les NTIC, ordinateurs, téléphones intelligents et autres objets connectés (tablettes, GPS, bracelets, montres, haut-parleurs, etc.), en plus des logiciels et applications associés, occupent aujourd'hui une place prépondérante dans les activités quotidiennes des individus.

Au fil des années, non seulement nous avons pu observer la montée en popularité de l'informatique, mais aussi des appareils technologiques de plus en plus personnalisés. La personnalisation sous-entend le fait de donner un caractère personnel à une abstraction, à quelque chose (CNRTL, s. d.). Dans le cas qui nous intéresse, nous parlons d'appareils qui sont personnalisés afin de s'intégrer aux habitudes de vie des individus. Notons par exemple l'iPhone, lancé en 2007 par Apple, un téléphone intelligent muni d'un écran tactile qui permet de téléphoner, de texter, de photographier et de naviguer sur Internet et d'avoir recours à plusieurs applications mobiles (cartes routières, bourse, etc.) (Ici Radio-Canada, 2017). Les individus sont invités à personnaliser l'écran de leur iPhone en téléchargeant des applications mobiles selon leurs champs d'intérêt. Par ailleurs, les avancées technologiques en sécurité permettent depuis peu la personnalisation de l'écran de verrouillage de l'iPhone. Ainsi, au-delà du simple code, il y a possibilité de l'emploi d'une empreinte digitale (Touch ID en 2013) ou de la reconnaissance faciale (Face ID en 2017), soit des éléments fondés sur des caractéristiques propres et uniques à chaque individu.

L'émergence des médias socionumériques, notamment la création de Facebook en 2004, YouTube en 2005 et de Twitter en 2006, permet aux individus de pouvoir « participer de manière active à la production de contenus médiatiques propres » (Proulx et Choon, 2011 : 105). Avec les appareils mobiles (téléphone, tablette, etc.), les individus peuvent s'exprimer en ligne à partir de n'importe où et à tout moment. Cela coïncide avec l'état d'esprit hyperindividualiste qui se manifeste par « l'émergence d'un individu qui prétend advenir par et pour lui-même, en dehors

de toute influence d'autorité morale, disciplinaire ou idéologique » (Mondoux, 2011 : 52). L'individu se sent de plus en plus autonome dans ses choix ayant accès à une gamme de produits de consommation personnalisés. Il voit dans les appareils technologiques et par le fait même, les médias socionumériques, la possibilité de façonner son identité et de pouvoir s'exprimer librement, sans contrainte :

> Voilà qui explique, d'une part, la trajectoire historique des technologies de l'information et de la communication (TIC) qui au cours des 40 dernières années sont devenues des outils individuels, et d'autre part, pourquoi ces outils, plus explicitement avec les médias sociaux, sont devenus des lieux d'expression personnelle. (*Ibid.*, 2011 : 52)

Durant cette même période, certains penseurs constatent implicitement ce qui pourrait être la fin de l'âge politique (Parsons, Deutsch et Easton cités par Birnbaum, 1975). Nous parlons ici du politique et non de la politique. Le politique étant « les conditions du vivre ensemble [et la] politique, [...] les stratégies de la conquête et de l'exercice du pouvoir » (Wolff, 2015). Les gouvernements qui dirigent et administrent la société le font avec « le consentement passif de citoyens apolitiques absorbés par leurs activités personnelles » (Favre, 1975 : 565). C'est ce qu'appelle le philosophe français Gilles Lipovetsky « l'ère du vide », où la société dans laquelle nous vivons « n'a plus d'idole ni de tabou, plus d'image glorieuse d'elle-même, plus de projet historique mobilisateur » (Lipovetsky, 1983 : 12). Ce sentiment de vide que reflètent les individus est, en d'autres mots, attribuables aux habitudes créées par les ressources matérielles informatiques qui les attirent et les entourent :

> Le procès de personnalisation impulsé par l'accélération des techniques, par le management, par la consommation de masse, par les médias, par les développements de l'idéologie individualiste, par le psychologisme, porte à son point culminant le règne de l'individu, fait sauter les dernières barrières. (*Ibid.*, 1983 : 35-36)

L'hyperconsommation se joint à l'hyperindividualisme, où les individus sont portés et absorbés par le plaisir de consommer, et ce, dans toutes les sphères de leur vie, ce qui les conduit vers « un futur immédiat de la rentabilité » (Citot, 2004 : 185).

Pourtant, les individus ne font pas seulement s'exprimer lorsqu'ils interagissent sur les médias socionumériques, ni uniquement consommer lorsqu'ils naviguent sur le Web ou consultent une application mobile : ils consultent des écrans. Avant même l'écran de lumière bleue ou l'écran cathodique, le terme « écran » pouvait être employé à l'époque comme « paravent ». Il s'agissait d'un objet servant d'intermédiaire pour protéger ou dissimuler comme « l'écran de fumée [d'une armée] qui cache et protège le mouvement des troupes qui s'activent derrière lui » (Galinon-Mélénec et Zlitini, 2013 : 8). Derrière les écrans des appareils connectés se cachent des dispositifs de traitements, de calculs et de retranscriptions numérisées des activités en ligne des individus. Les usagers sont devenus en quelque sorte des producteurs de traces numériques (*Ibid.*, 2013 : 11). La migration de bon nombre de leurs activités quotidiennes vers le numérique a entraîné « la production massive de traces, autant de résidus de nos opérations sans cesse plus nombreuses dans un monde de plus en plus numérisé » (Bonenfant et coll., 2015 : 34).

Ces traces peuvent être produites volontairement par les usagers comme, par exemple, lorsqu'un usager sur Facebook publie en ligne un texte, une image, une vidéo ou s'exprime de toute autre façon (commenter ou aimer une publication, aimer une page d'une organisation, etc.). Or, cela constitue seulement une partie des traces numériques pouvant être générées. De fait, une grande majorité de ces traces sont produites involontairement. L'usager qui souhaite créer une publication sur Facebook, ouvre l'application mobile sur son téléphone intelligent, prend un moment pour consulter deux ou trois nouvelles de ses amis ou des pages qu'il suit, pour enfin quitter l'application. Les traces involontaires peuvent alors correspondre au temps passé à regarder l'application (heure de début et de fin), sa position géographique lors

de sa consultation, ses intérêts en fonction des nouvelles qu'il a lues. Évidemment, l'usager ne partage pas toutes ces informations avec son réseau sur Facebook. Il s'agit donc d' « une conséquence acceptée, plus ou moins consciemment, de l'usage des technologies numériques qui génèrent de facto des traces » (*Ibid.*, 2015 : 34).

Pour ceux qui désirent utiliser des appareils technologiques sans produire de traces, cela nécessite « des compétences informatiques certaines – voire suspectes (comme l'encryptage[2]) » (*Ibid.*, 2015 : 34). Alors, les individus continuent à produire des traces numériques qu'ils le veuillent ou non. Dans l'ombre, nous avons affaire à un « enregistrement massif et systématique » (Rouvroy et Berns, 2010 : 88) de toutes ces traces qui sont ensuite emmagasinées dans des centres de stockage et gérées par des entreprises privées.

La présence en ligne – pages Web consultées, applications mobiles utilisées, publication de contenu sur les médias socionumériques – produit de plus en plus de traces sous forme de données (Rouvroy, 2016 : 4-6). Au sens étymologique, le terme « donnée » provient du terme latin *datum*, lui-même dérivé du verbe *dare* qui veut dire « donner ». Nous parlons ici de données qui sont cédées. Toutefois, certains chercheurs (Jensen, 1950 ; Borgman, 2007 ; Kitchin et Dodge, 2011, cité dans Kitchin, 2014 : 2) remettent en cause l'origine de ce mot : nous ne faisons plus l'action de donner, mais plutôt celle d'extraire des données. En ce sens, le terme « donnée » s'inspire davantage du mot latin *capta* qui veut dire « prendre », des données qui sont prises (*Ibid.*, 2014 : 2). Le phénomène des mégadonnées est venu confirmer ce principe d'extraction. Apparues au milieu des années 1990 (Diebold, 2012 : 3), les mégadonnées réfèrent à la manipulation et l'analyse en temps réel d'un ensemble de données à grande échelle « provenant de sources variées [et] utilisant des

[2] Notamment avec l'utilisation d'un logiciel de sécurité permettant le chiffrement ou le cryptage de données. Ce procédé permet de chiffrer une information, soit de la rendre inaccessible à toute personne qui ne possède pas la « clé » (ou la solution secrète) pour déchiffrer ladite information.

algorithmes très puissants pour dégager les constantes sous-jacentes et les corrélations afin de prédire les résultats à venir » (Commissariat à la protection de la vie privée du Canada, 2014).

Dans la littérature, les mégadonnées sont également décrites par cinq « V » (volume, variété, vélocité, véracité et valeur) (Ménard et Mondoux, 2018 : 224). Le volume est l'abondance des données qui sont collectées et traitées : l'univers numérique serait composé aujourd'hui de plus de 1 200 milliards de milliards d'octets[3] dont 90 % auraient été produits dans les deux dernières années (Rouvroy, 2016 : 4-5). En termes de variété, les données proviennent d'une multitude de sources :

> les hard data [...] produites par les institutions et administrations publiques [...] [, les] soft data [,] les données émises par les individus, soit intentionnellement, à travers les blogs, réseaux sociaux, forums de discussion, soit involontairement [...] à travers des dispositifs de trajectoires en ligne, de vidéosurveillance, localisation GPS, de suivi des flux de circulation, d'imagerie satellitaire, d'enregistrement des transactions bancaires. (*Ibid.*, 2016 : 6-7)

La vélocité se veut « la vitesse à laquelle [les données] sont accumulées en temps réel » (*Ibid.*, 2016 : 9). La véracité porte, quant à elle, sur la considération des données comme étant le « réel ». Les mégadonnées automatisent en temps réel la récolte et l'analyse de données, c'est-à-dire qu'elles prétendent éliminer toute forme de médiation et ainsi « [forent des] données ''brutes'' en guise d'un ''réel'' » (Ménard et Mondoux, s. d. : 2). Bien que certaines compagnies informatiques comme IBM vantent les mérites d'un bon nettoyage pour ne garder que les données de qualité (Wired, 2013), plusieurs questions demeurent en suspens quant

[3] L'octet est l'unité numérique qui permet de coder un caractère (Rouvroy, 2016 : 4 ; CNRTL, s. d.). Si la tendance se maintient d'ici 2020, le chiffre de 1 200 milliards de milliards d'octets pourrait décupler et atteindre plus de 44 zettaoctets (un zettaoctet correspond à 1 000 000 000 000 000 000 000 octets) (*op. cit.*, Rouvroy, 2016 : 5).

à la fiabilité et l'utilité de ces données « nettoyées »[4]. À cet effet, le philosophe français Bernard Stiegler soulève l'exemple de la crise financière des prêts à haut risque en 2007, où « les données entrées dans les modèles de gestion des risques ne provenaient généralement que des deux dernières décennies, qui furent une période d'euphorie » (Stiegler, 2015 : 11). L'effondrement du marché boursier s'en est suivi, et ce, même avec des « robots supposés ''objectiver'' le réel » (*Ibid.*, 2015 : 11).

Enfin, la valeur est sans doute l'une des caractéristiques les plus recherchées par les entités tierces qui, par le croisement de données ou la gestion d'algorithmes, forment un circuit marchant et mettent à profit les données des usagers (ex. : profilage publicitaire, assurance et pointage de crédit, etc.) (International Working Group on Data Protection in Telecommunications, 2014 ; Ménard et Mondoux, s. d. : 4). Âge, sexe, langue, situation géographique, intérêts, comportements en ligne, appareils… des données aussi variées et monnayables sont récoltées sur les usagers, notamment avec le logiciel d'analyse d'audience Google Analytics (voir Annexe 1). Pour les agences et les régies publicitaires, ces données permettent notamment de créer des publicités plus personnalisées et plus pertinentes dans le but d'inciter les usagers à consommer.

Les deux dernières caractéristiques, la véracité et la valeur remettent en cause la neutralité même des mégadonnées, et ce, à plusieurs niveaux. Sur le plan technique, les centres de données récoltent des données dites « vraies » comme ils sont « conçus pour retenir certains types de données et permettre certains types d'analyse[5] » (Kitchin, 2014 : 21). En finance, par exemple, les données sont catégorisées en un « profilage minutieux des comportements individuels » pour le

[4] Par ailleurs, le philosophe français Jean-François Lyotard remettait déjà en doute à la fin des années 1970 les autorisations remises à IBM pour le lancement en orbite de satellites de communication et de banque de données : « Qui y aura accès ? Qui définira les canaux ou les données interdits ? Sera-ce l'État ? Ou bien celui-ci sera-t-il un usager parmi d'autres ? » (Lyotard, 1979 : 8).

[5] Traduction libre

marketing et la publicité ciblée (Arpin-Simonetti, 2015). L'objectif est d'attribuer une valeur à ces données et de « déterminer d'avance les volontés particulières par des mécanismes de planification de la consommation » (Ouellet, 2015). Ainsi, des régies publicitaires peuvent mettre en place des algorithmes spécifiques permettant de constituer des profils prédictifs à partir de quelques données (âge, position géographique, etc.) et du comportement en ligne (ex. : pages Web consultées), permettant de déduire avec une grande probabilité que tel usager sera amené à cliquer sur telle publicité. Autre exemple, dans le domaine politique, l'Agence nationale de la sécurité américaine (NSA) a un accès privilégié aux données amassées par les géants de la Silicon Valley (Google, Facebook, etc.), ce qui permet au gouvernement de « [mettre] à profit les outils de profilage développés par l'industrie » (*op. cit.*, Arpin-Simonetti, 2015).

Bien que, pour certains, l'analyse des mégadonnées peut servir à acquérir de nouvelles connaissances et à résoudre plus efficacement des problèmes complexes (IBM, s. d.), ce procédé peut également soulever des enjeux éthiques et avoir des conséquences négatives, dont particulièrement l'atteinte à la vie privée (Metcalf et Crawford, 2016 ; Zimmer, 2010 ; Rouvroy, 2016). La professeure américaine et spécialiste en science de l'information Helen Nissenbaum et son collègue expliquent notamment en quoi les mégadonnées peuvent affecter les valeurs fondamentales de l'être humain :

> Là où ces données s'engagent à enregistrer des détails sur le comportement humain, elles ont été perçues comme une menace pour les valeurs fondamentales, allant de l'autonomie à l'équité, en passant par la justice, le respect de la procédure, la propriété, la solidarité et peut-être la plus grande partie de la vie privée[6]. (Barocas et Nissenbaum, 2014 : 44)

[6] Traduction libre

C'est pour cette raison que la plupart des entreprises privées et leurs partenaires (ex. : régies publicitaires) tentent de recourir à des méthodes comme l'anonymisation[7] des données qu'elles récoltent afin de protéger l'aspect privé de ces dernières. Toutefois, comme le montre l'étude de De Montjoye et ses collaborateurs (2015) sur les achats par carte de crédit aux États-Unis, il suffit de quatre données spatiotemporelles[8] « même ''anonymisées'' » pour identifier 90 % des membres d'un groupe d'individus. Dans la même veine, le chercheur Andreas Dewes et la journaliste Svea Eckert de *The Guardian* (2017) ont réussi à dévoiler des données « anonymes » de plus de 3 millions de citoyens allemands en se procurant gratuitement ces données. En créant une fausse compagnie de marketing, ils ont eu accès à l'historique de navigation d'un grossiste de données. Par exemple, il était facile d'identifier un usager qui visitait sa propre page Twitter contenant l'identifiant dans l'adresse du site Web. Sinon, par la corrélation de données :

> 10 adresses [pouvaient] être suffisantes pour identifier quelqu'un – pensez, entre autres, au peu de gens qui travaillent dans votre entreprise, ont un compte dans votre banque, pratique votre loisir, lisent votre journal favori et utilisent votre fournisseur de téléphonie cellulaire. (Pieuvre, 2017)

Par ailleurs, même si des individus veulent et font des efforts pour rester anonymes sur Internet, leurs données peuvent être dévoilées, avec des moyens parfois jugés inappropriés. C'est le cas de chercheurs britanniques qui ont réussi à identifier Banksy, l'un des plus célèbres artistes anonymes de l'art urbain (Hauge et coll.,

---

[7] Le procédé qui permet d'anonymiser, de préserver l'anonymat des données provenant, par exemple « des applications de téléphones mobiles, des *smart grids*, des transpondeurs intégrés aux véhicules [...], des dossiers médicaux, des données de localisation, des réseaux sociaux, des registres de passagers des transports aériens, des registres publics, des programmes de fidélité, des séquençages génomiques, des historiques d'achats, mais aussi, de plus en plus, d'une quantité d'objets ''intelligents'' [...] qui permettent non seulement d'identifier leurs propriétaires, mais sont en plus très révélatrices de leurs modes de vie » (Rouvroy, 2016 : 23).

[8] Les données spatiotemporelles peuvent être le lieu, la date et le montant des achats effectués (De Montjoye et coll., 2015).

2016)[9]. Bien que toutes les données utilisées par les chercheurs aient été publiques, les méthodes employées (profilage géographique, algorithme, etc.) pour retrouver l'individu ont été critiquées par d'autres chercheurs : « Même anonymes, les ensembles de données publiques peuvent produire des dommages selon la façon dont ils sont utilisés[10] » (Metcalf et Crawford, 2016 : 27).

En plus des risques d'identification, les mégadonnées peuvent conduire à des formes de surveillance. Après les révélations d'Edward Snowden en 2013 sur l'accès de l'Agence nationale de la sécurité américaine (NSA) à l'ensemble des données amassées par les géants de la Silicon Valley (Google, Facebook, etc.) (Greenwald et MacAskill, 2013), une enquête réalisée par le Pew Research Center (2015) a révélé qu'environ un Américain sur trois avait effectué une action visant à rendre ses données plus privées. Au Québec, nous avons été récemment interpellé par cette question quand le président des États-Unis, Donald J. Trump, a signé un décret visant les agences gouvernementales et leurs politiques en matière de vie privée pour exclure les personnes vivant à l'extérieur du pays des protections offertes par le *Privacy Act* (loi sur la protection de la vie privée)[11] en ce qui a trait aux informations à caractère personnel (The White House, 2017). Or, les experts estiment qu'environ 90 % du trafic en ligne effectué par les Canadiens passent par des sites américains (Tencer, 2017). Ainsi, « un courriel envoyé de Vancouver à Montréal peut voyager à travers plusieurs villes des États-Unis, où il peut être surveillé par différents points d'écoute de la NSA[12] » (OpenMedia, 2017). Cela peut amener la population

[9] En ayant recours au profilage géographique, c'est-à-dire une technique mathématique développée en criminologie pour retracer un délinquant, les chercheurs ont pris en compte les différents emplacements des œuvres de l'artiste. Ils ont ensuite calculé la probabilité que ces œuvres soient reliées à une résidence dans la zone des emplacements fréquentés. Ils ont enfin mis en évidence un candidat potentiel à l'identité réelle de Banksy.

[10] Traduction libre

[11] Adoptée en 1974, il s'agit du « principal cadre juridique protégeant les données à caractère personnel détenues par le secteur public aux États-Unis » (De Hert et Bellanova, 2008).

[12] Traduction libre

québécoise à s'intéresser davantage au traitement des données qui s'effectue présentement chez ses voisins du Sud.

1.2. Revue de la littérature

Les techniques utilisées par les entreprises privées des NTIC pour collecter des données peuvent représenter des enjeux importants et des risques d'atteinte à la vie privée des usagers. La sécurité informatique peut être une piste pour rehausser la protection de la vie privée en ligne.

1.2.1.Des solutions individuelles pour protéger la vie privée

Nous pourrions penser que l'individu se doit simplement d'adopter de bonnes habitudes pour protéger sa vie privée sur Internet. Le Commissariat à la protection de la vie privée du Canada fournit en ce sens 10 conseils visant à aider les individus à mieux protéger leur vie privée :

> Pensez-y deux fois, posez des questions, exprimez-vous sur le respect de la vie privée, refusez tout simplement, protégez votre numéro d'assurance sociale, protégez vos appareils, protégez vos mots de passe, familiarisez-vous avec les paramètres de confidentialité, soyez prudent lorsque vous supprimez des renseignements, connaissez vos droits. (Commissariat à la protection de la vie privée du Canada, 2018)

Plusieurs de ces mesures sont applicables en ligne. Notamment, le Commissariat incite à protéger son ordinateur, téléphone ou autre appareil mobile à l'aide d'un mot de passe difficile à deviner, à télécharger la dernière version de logiciels (antivirus, antipourriels et pare-feu) et à désactiver les fonctions Wi-Fi et Bluetooth lorsque non

requises. De plus, le Commissariat invite les usagers à se familiariser avec les paramètres de confidentialité, indiquant qu'il est possible, dans la plupart des cas, de les modifier afin de déterminer les renseignements personnels à rendre public. Enfin, le Commissariat encourage les individus à prendre l'habitude de lire les politiques de confidentialité des sites et applications mobiles qu'ils utilisent.

Cependant, deux chercheurs américains avaient estimé en 2012 à 76 jours de travail pour lire l'étendue des conditions d'utilisation des sites Web qu'ils visitaient et des applications qu'ils utilisaient durant une année (McDonald et Cranor, 2008 ; Madrigal, 2012). Ainsi, lorsque les usagers acceptent les conditions d'utilisation, ils ne sont pas nécessairement conscients de leur contenu. Dans bien des cas, elles sont présentées de façon à ne pas être lues : une abondance de mots, de lignes, de pages, une petite police, des phrases longues, complexes et issues d'un vocabulaire juridique. Les entreprises privées technologiques « ont tendance à imposer unilatéralement les termes du contrat [...] dans l'espoir que les internautes vont simplement accepter ces conditions, par nécessité ou l'indifférence » (De Filippi, 2016 : 6). D'un côté, le Commissariat invite à se familiariser davantage aux conditions d'utilisation et aux politiques de confidentialité et, de l'autre côté, des chercheurs observent la difficulté et l'incapacité des usagers à y arriver.

Le Commissariat propose également aux individus « de refuser tout simplement » de divulguer des données. Ainsi, « si l'usager pense que ces données peuvent révéler des informations sensibles qui ne sont pas censées être partagées, il peut simplement refuser de fournir ces données[13] » (Mehmood et coll., 2016 : 1824). Toutefois, le professeur et chercheur américain en droit Solove (2012) affirme que les individus ne sont pas en mesure de gérer eux-mêmes leur vie privée en ligne de manière appropriée, car ils font face à trois problèmes structurels. Le premier est un problème

[13] Traduction libre

d'échelle. L'individu peut être capable de gérer ces paramètres de confidentialité avec seulement quelques entreprises, mais pas la majorité. Selon Solove, l'Américain moyen visite près de cent sites par mois et fait affaire avec une panoplie de compagnies qui produisent des données (commerçant, assureur, banque, etc.). Le second est un problème de corrélation. Même si un individu fait des choix éclairés pour restreindre ces données, il a du mal à comprendre comment celles-ci peuvent être utilisées dans le futur, par exemple avec la corrélation possible de ses données avec d'autres données. À cet effet, une récente étude de la chercheuse torontoise Austin et de son équipe (2018) a réussi à montrer que 757 applications mobiles sur le système d'exploitation Android collectaient en moyenne 60 % plus de données que ce que les politiques de confidentialité indiquaient. Le troisième et dernier problème énuméré par Solove est celui de l'évaluation. Les individus privilégient les avantages à court terme (ex. : accès à des sites Web ou des applications mobiles) sans nécessairement évaluer s'il peut y avoir des conséquences sur leur vie privée.

En résumé, nous comprenons que les individus se retrouvent dans une impasse face à la prise en charge de leur vie privée en ligne. Bien que les conditions d'utilisation et les politiques de confidentialité soient souvent disponibles, les individus se retrouvent submergés d'informations qu'ils ne comprennent pas nécessairement et qu'ils acceptent par manque de temps ou de connaissance. Voyons maintenant de plus près si certaines des solutions techniques qui figurent dans les conseils du Commissariat peuvent alors conduire à une meilleure protection.

1.2.2.Des solutions techniques pour protéger la vie privée

Les individus peuvent être amenés à utiliser des solutions techniques pour chercher à protéger leur vie privée en ligne, c'est-à-dire d'autres technologies, tels des logiciels ou des applications, leur permettant de mieux contrôler les traces qu'ils produisent. Les usagers peuvent notamment télécharger des « extensions anti-pistage, des bloqueurs de publicités ou des scripts et des outils de cryptage[14] » (Mehmood et coll., 2016 : 1824).

En ce sens, la chercheuse américaine Roesner et ses collaborateurs (2012) ont effectué une étude sur les sites Web qui utilisent des outils de suivi[15] sur les usagers. À partir d'une liste des 500 meilleurs sites selon Alexa, un site d'analyse de trafic sur Internet, les chercheurs ont évalué différentes stratégies de défense contre le suivi. Les technologies observées (blocage de témoins de connexion et de fenêtres intruses) peuvent s'avérer efficaces pour une grande majorité de sites Web, mais aucun mécanisme ne semble être très efficace sur les sites populaires tels que Facebook, Twitter et Google+[16]. Les chercheurs ont aussi trouvé qu'avec l'ajout d'un module de partage[17] sur n'importe quel site Web, certains médias socionumériques peuvent suivre et récolter des données sur les usagers même si ceux-ci n'ont pas activé le partage du contenu. Par exemple, la figure 1.1 montre la façon dont Facebook place un témoin de connexion d'identification sur un utilisateur (1) par l'entremise du bouton « J'aime ». En effet, « lorsqu'un site intègre un tel bouton, la demande à Facebook pour fournir ce bouton (2)(3) inclut un témoin de connexion. [...] Cela

---

[14] Traduction libre

[15] Par exemple, une entreprise privée pourrait suivre et récolter des données sur les habitudes de navigation d'un usager pour ensuite lui proposer des publicités ciblées.

[16] Google a annoncé la fermeture de Google+ en avril 2019 en raison d'une chute de popularité.

[17] Il existe de nombreux modules de partage dont les boutons « J'aime » de Facebook, « Tweet » de Twitter et « +1 » de Google+.

permet à Facebook de suivre l'utilisateur sur n'importe quel site qui intègre un tel bouton[18] » (*Ibid.*, 2012 : 5).

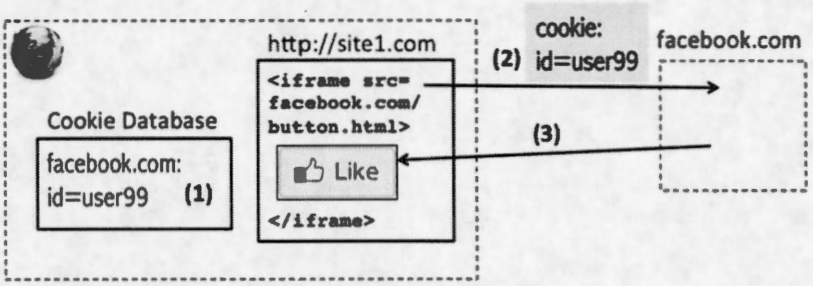


Figure 1.1 – Module du bouton « J'aime » de Facebook (Roesner et coll., 2012 : 4)

Dans le cadre de leur étude, Roesner et ses collaborateurs ont donc créé l'extension *Share me not* pouvant être ajoutée à un navigateur Web et empêchant ce type de suivi. Cette technologie leur a permis d'éliminer entièrement le nombre de suivis sur Twitter, mais ils n'ont pas réussi à supprimer la totalité des suivis sur Facebook et Google+ (bien qu'ils en aient réduit l'importance). Cela démontre à quel point certaines entreprises de médias socionumériques exercent des rapports de pouvoir qui font pencher l'équilibre en leur faveur, de par leurs techniques de programmation avancée qui permettent d'emmagasiner de l'information, et ce, même auprès des usagers qui cherchent à les contourner.

En suivant le même raisonnement, les chercheurs américains Howe et Nissembaum ont tenté de réduire le nombre de suivis en ligne par la création d'*AdNauseam*. Cette extension pour navigateur[19] permet de simuler automatiquement « des clics (ou des visites) sur les annonces collectées, avec l'intention de s'afficher sur le serveur du site Web (ainsi que les réseaux publicitaires)[20] » (Howe et Nissenbaum, 2017 : 4). Cela

[18] Traduction libre
[19] Un module d'appoint offrant des fonctions supplémentaires au navigateur.
[20] Traduction libre

entraîne l'obscurcissement du profil de l'usager et complique le suivi en ligne par les annonceurs. Un des risques associés à cette extension était l'augmentation du nombre de suivis par les annonceurs. Néanmoins, les chercheurs ont observé le contraire en comparant *AdNauseam* à d'autres extensions similaires (Adblock Plus, uBlock et Privacy Badger). Après des tests effectués sur des sites Web, *AdNauseam* a généré moins de témoins que le non-usage d'une extension. De plus, il a mieux performé que l'extension la plus connue Adblock Plus, mais moins qu'uBlock en raison de la nécessité de faire apparaître les publicités pour pouvoir fonctionner. En 2017, le géant informatique Google a désactivé *AdNauseam* sur Google Chrome, le navigateur le plus populaire dans le monde, forçant les chercheurs à développer une nouvelle version de leur extension qui est encore disponible aujourd'hui (AdNauseam, 2017).

Somme toute, des solutions techniques tendent à vouloir donner plus de pouvoir aux individus afin qu'ils puissent mieux protéger leur vie privée en ligne. Néanmoins, nous observons que ces solutions ne sont pas encore parfaites. Lors de la mise en place des extensions *Share me not* et *AdNauseaum*, nous remarquons également des tensions entre les usagers qui désirent réduire le nombre de données et les sites Web et les annonceurs qui désirent continuer à les cumuler.

1.2.3.Question générale de recherche

Nous n'avons pas l'impression que les individus doivent recourir seulement à des solutions techniques ou individuelles pour bien protéger leur vie privée en ligne. Certes, les individus peuvent changer des paramètres de confidentialité ou utiliser un logiciel de sécurité, mais comme nous l'avons vu, ces gestes ou ces outils ne permettent pas de protéger entièrement leurs renseignements personnels en ligne. Au fond, ils continuent à profiter des bienfaits de l'univers numérique sans le remettre en question. En général, ces solutions nous ramènent seulement au point de vue

individuel, soit la capacité de l'individu à prendre des moyens pour gérer sa vie privée. Or, le questionnement autour de la vie privée ne touche pas simplement l'individu. Nous croyons que nous devons avoir une vision plus élargie et plus globale de la vie privée.

À cet effet, le chercheur québécois Ménard et ses collègues (2016) ont analysé le circuit marchand des médias socionumériques en tant que « processus d'industrialisation du traitement des données personnelles ». Le circuit marchand ne peut avoir lieu qu'avec la participation de tous les individus qui produisent des données volontairement ou involontairement, et ce, de manière collective. Les individus créent des mégadonnées qui ont une valeur. Ces mégadonnées représentent des marchandises qui circulent au sein d'une société marchande, où elles deviennent « les réels sujets de l'activité sociale » (Ouellet et coll., 2016 : 599). Ainsi, les individus alimentent le circuit marchand qui demande à être nourri. Nous pouvons notamment faire un parallèle avec l'ouvrage *Le capital* du philosophe allemand Karl Marx, où l'ouvrier du 19e siècle devient moteur de la machine qu'il alimente :

> Dans la manufacture et le métier, l'ouvrier se sert de son outil ; dans la fabrique il sert la machine. Là le mouvement de l'instrument de travail part de lui ; ici il ne fait que le suivre. Dans la manufacture les ouvriers forment autant de membres d'un mécanisme vivant. Dans la fabrique ils sont incorporés à un mécanisme mort qui existe indépendamment d'eux. (Marx, 1867 : IVe section, chapitre XV)

Ce circuit marchant présente également des rapports de pouvoir. Tout en haut de l'échelle, nous retrouvons les patrons, les grandes compagnies technologiques comme le GAFAM (Google, Amazon, Facebook, Apple et Microsoft), qui gèrent et contrôlent ce circuit de façon à générer le plus grand nombre de mégadonnées possibles. Plus bas dans l'échelle, nous retrouvons les ouvriers, des usagers qui produisent des données en navigant dans les trajectoires dessinées et imposées par les GAFAM.

Les usagers peuvent peut-être réduire leurs traces numériques par une meilleure compréhension de leurs paramètres de confidentialité ou l'usage de solutions techniques, mais les entreprises du GAFAM continueront tout de même de manière générale à recueillir des données sur leur comportement. Alors, qu'en est-il des usagers qui souhaitent reprendre un peu plus de contrôle sur leurs données et par conséquent sur leur vie privée ? Par la collaboration des GAFAM avec les agences gouvernementales (révélé par l'affaire d'Edward Snowden en 2013), le circuit marchand dessert aussi les intérêts du gouvernement. Dans ce contexte, est-il possible de s'opposer à ce circuit marchand ? Est-il possible également de modifier ces rapports sur la seule base des actions individuelles ?

Cela nous amène à notre question générale de recherche : **dans un tel contexte, comment Crypto.Québec peut-il affecter, modifier ou détourner les rapports de pouvoir du circuit marchand des mégadonnées induits par les GAFAM ?**

CHAPITRE 2

CADRE THÉORIQUE

Dans ce deuxième chapitre, nous présentons les théories qui nous permettent de mieux comprendre et d'orienter la problématique présentée. Cela est suivi des questions et des hypothèses spécifiques de notre recherche. Pour commencer, nous nous intéressons aux théories du penseur québécois Michel Freitag qui peuvent nous être utiles pour mieux comprendre le circuit marchand des mégadonnées.

2.1. Les modes de reproduction de la société

Considéré comme un « géant de la sociologie » au Québec (Baillargeon, 2009), le sociologue Michel Freitag a cherché à définir la société actuelle avec de nombreux ouvrages sur la sociologie dialectique. En quelques mots, la sociologie dialectique de Freitag est une manière de concevoir « les sociétés réelles comme une structure hiérarchique de différents modes de reproduction » (Filion, 2006 : 170). La reproduction de l'espèce humaine – en d'autres termes, la transformation de la société dans le temps – est décrite dans ce concept freitagien « sous trois modes particularisés de reproduction : culturel-symbolique, politico-institutionnel et décisionnel-opérationnel » (*Ibid.*, 2006 : 166-167). Le mode de reproduction de la première concerne la société mythique, la seconde, les sociétés féodales et modernes et la dernière, la société postmoderne (*Ibid.*, 2006 : 175).

La première société à mode de reproduction « culturel-symbolique » est caractéristique des communautés primitives. Dans ces sociétés, la régulation des pratiques sociales (vie quotidienne, famille, amitié) s'appuie sur une culture partagée par la communauté. Autrement dit, c'est le mythe d'origine qui oriente la société, c'est-à-dire « l'expérience significative enregistrée et accueillie comme légitime dans le cheminement de l'action à travers ses obstacles intérieurs et extérieurs » (*Ibid.*, 2006 : 188). Les individus primitifs peuvent être confrontés à des changements ou des conflits, mais ils préfèrent les éviter et rester fidèles au passé pour ne pas menacer l'existence de leur communauté. En effet, les individus « n'ont aucune distance critique à l'égard de la culture, ils baignent dedans et interprètent le sens des choses à travers elle » (Freitag et Bonny, 2002 : 32). Ils font même appel à des mécanismes (ex. : rituels et tabous) qui perpétuent le mythe d'origine.

Le second mode de reproduction « politico-institutionnel » a été développé à la fin du mythe d'origine, entre autres, par la recherche d'autonomie et l'acceptabilité des conflits. Les sociétés primitives sont passées d'un mode de vie nomade à sédentaire, de l'élevage à l'agriculture et de la possession d'une terre au droit à la propriété. Cela conduit l'individu vers une certaine autonomie vis-à-vis la communauté et amène de nouveaux défis. En effet, « le mythe n'arrive plus à justifier le rapport de force qui s'installe pour les droits de propriété et des produits du travail » (Martin, 2007 : 62). Ainsi, le mode de reproduction politico-institutionnel cherche à réguler les pratiques sociales « non plus par la médiation de la norme culturelle intériorisée, mais par celle de la règle imposée et sanctionnée en extériorité par un pouvoir » (*op. cit.*, Freitag et Bonny, 2002 : 40). Les pratiques sociales sont alors institutionnalisées et portées par des acteurs sociaux dominants qui exercent un pouvoir :

> Le pouvoir rétablit l'unité de la société par-delà les conflits d'orientation qui la traversent, sans toutefois abolir ceux-ci. D'un côté, il fait signe vers une domination sociale, à travers laquelle les orientations portées par les acteurs sociaux dominants sont imposées à l'ensemble de la société. De l'autre, il réalise l'unification et l'objectivisation de la société à travers le système juridique et l'ensemble des institutions qui encadrent et orientent les pratiques et rapports sociaux. (*Ibid.*, 2002 : 40)

L'élément distinctif et fondamental du mode de reproduction politico-institutionnel, c'est qu'il permet une « production réflexive des institutions et des règles sociales, à partir des grands principes et de finalités explicites, ce par quoi la *praxis*[21] politique s'élève au-dessus des simples rapports de force, les dépasse et les contient » (*Ibid.*, 2002 : 33). Par conséquent, Freitag distingue deux types d'institutions dans le mode de reproduction politico-institutionnel. Le premier cycle se déroule à l'époque médiévale des royaumes et des empires. Cette société s'appuie sur la tradition et la religion (un ou des dieux) pour orienter sa destinée. Les pratiques sociales sont donc institutionnalisées dans le respect de l'ordre divin.

Le second cycle s'inscrit dans l'époque moderne s'étalant de la fin du 19^{e} siècle au début du 20^{e} siècle (CNRTL, s. d.). Comparativement au premier cycle, la société dans le deuxième cycle se reproduit avec la mise en place d' « une structure sociale dans laquelle prennent forme certains conflits d'intérêts » (Beaupré, 2001 : 53). En ce sens, la société moderne rejette l'ordre divin pour le remplacer par des pratiques sociales institutionnalisées et réfléchies par la collectivité (*op. cit.*, Freitag et Bonny, 2002 : 34). La religion est alors détrônée par l'idéologie[22] des grands principes :

---

[21] La *praxis* est l'activité humaine réelle orientée vers son destin : « il s'agit de transformer le monde (projet ou fin) sur la base de la critique et de la connaissance de l'existant » (Sanchez-Vasquez, 1977 : 142).

[22] Contraction des mots latins *idéo* pour idée et *logie* pour théorie, l'idéologie était décrite au Siècle des Lumières comme étant la « science qui a pour objet l'étude des idées » (CNRTL, s. d.). Cette science cherche en quelque sorte à théoriser les théories dans un système total, une conception pratiquement parfaite (Quantin, 1987 : 191). Une notion qui sera par la suite critiquée par Karl Marx alors que « les idées dominantes d'une époque ne sont [pour lui] que les idées de la classe dominante » (*Ibid.*, 1987 : 192).

notamment la raison, la liberté et les droits de l'homme et du citoyen (Filion, 2006 : 175). Ainsi, la société moderne se reproduit dans le temps avec un objectif commun, collectif et de société qui est d'assurer le « meilleur des mondes possibles » (Filion, 2010 : 78).

Il est à noter que Freitag aborde la reproduction sociétale à travers les types de médiations, dont les médiations transcendantales qui se trouvent au-dessus de l'individu, c'est-à-dire « un tout qui fonctionne et se reproduit par le sens » (Gendreau-B., 2009 : 49). Si la société « politico-institutionnelle » du premier cycle est guidée par un transcendant (un ou des dieux), le second cycle, lui, rejette la religion en s'orientant plutôt par une référence transcendantale (les grands principes). Par conséquent, la société moderne est dotée de valeurs communes et institutionnelles, et c'est ainsi que les pratiques sociales transcendent et se reproduisent dans le temps puisqu'elles sont institutionnalisées par « la constitution d'une superstructure d'institutions politiques et juridiques » (Filion, 2006 : 167).

Depuis la fin des années 80, la société postmoderne présente un modèle de reproduction « décisionnel-opérationnel », où nous assistons à l'occultation des médiations symboliques transcendantales par l'expansion du capitalisme. Pour le sociologue Freitag, il s'agit du mode de reproduction opposé au mode politico-institutionnel qui est plus difficile à cerner que ces précédents, car il décrit la « réalité actuelle » (*Ibid.*, 2006 : 251, 253). Alors que le mode de reproduction politico-institutionnel était porté par une science classique, où régnaient les décisions rationnelles et objectives, la science actuelle tend vers l'efficacité, le contrôle et la prévision des opérations sur le réel (*Ibid.*, 2006 : 45-46). Cette compréhension critique de la société est notamment influencée par la mutation de la science à la technoscience : les « problèmes engendrés par une société [...] [dirigée] par des promoteurs d'une idéologie technocratique [...] a pour effet immédiat de favoriser le libre surgissement d'ordres capitalistiques spontanés » (*Ibid.*, 2006 : 88). Ce faisant,

la logique capitaliste et marchande s'impose dans toutes les facettes du mode de reproduction actuel. Les décisions qui y sont prises sont pour la plupart d'ordre économique. Motivées par l'argent, elles doivent être calculables et mesurables (*Ibid.*, 2006 : 169, 256).

Tout ce qui concerne les théories et pratiques du passé est remplacé par « des médiations culturelle et institutionnelle en information cybernétique, neutre, quantifiable et efficiente » (*op. cit.*, Filion, 2006 : 169). De fait, Freitag n'est guère optimiste sur l'avenir de la société lorsqu'il écrit que le mode de reproduction décisionnel-opérationnel peut se légitimer lui-même. Il « n'a pas besoin [...] de se limiter et de s'orienter par une référence transcendantale, puisqu'il considère le réel comme la somme des problèmes empiriques qu'il a à gérer de manière technico-économique » (*Ibid.*, 2006 : 262). En d'autres mots, le mode de reproduction se valide par lui-même sans même avoir à remettre en question son *modus operandi* – son fonctionnement –, notamment par les écrits du passé. Passant de l'idéologie des grands principes à l'idéologie de l'efficacité technique, le mode de reproduction décisionnel-opérationnel vise « un rapport immédiat au monde sans réflexivité ni sens » (*op. cit.*, Baillargeon, 2009). Comme le font remarquer Ménard et Mondoux (s. d. : 11), cela peut s'appliquer aux relations sociales où celles-ci sont délaissées, remplacées et supplantées par des opérations purement mathématiques :

> Les concepts de communication et d'information subissent en effet dans le champ des nouvelles technologies informatiques une mutation radicale de leur sens : les réalités qu'ils désignent spécifiquement ne sont plus d'ordre symbolique et culturel, mais technique et opérationnel. (Freitag, 2003 : 7)

En ce sens, le mode de reproduction décisionnel-opérationnel réduit le langage « en information formalisée, quantifiable et monnayable, [...] la valeur d'un simple code » (*op. cit.*, Filion, 2006 : 264). Ce qui fait en sorte que le sens de la communication n'est plus le même, désignant « directement les intérêts ou

motivations spécifiés par leurs seules divergences circonstancielles » (*Ibid.*, 2006 : 264).

Par exemple, les entreprises du GAFAM réduisent le comportement de leurs usagers en de simples unités de mesure informatiques. Ces structures, ces systèmes, ces opérations, ces dynamiques de régulation jouent le rôle de « médiation généralisée [...] qui finit par s'imposer comme la forme la plus évidente, la plus contraignante de la réalité » (*op. cit.*, Freitag et Bonny, 2002 : 111). Des habitudes de navigation sur Internet aux mots-clés insérés dans un moteur de recherche, toutes ces données peuvent être captées, analysées et vendues à des fins publicitaires, car elles semblent décrire la « vraie » réalité de leurs usagers. Non seulement ces données peuvent servir aux publicitaires, mais elles peuvent également avoir de plus grandes visées. Ce sont des connaissances qui peuvent être détenues par un État aux dépens des autres pays dans une compétition mondiale pour le pouvoir. Comme le prédisait le philosophe français Jean-François Lyotard dans *La Condition postmoderne*, les États « se sont battus pour maîtriser des territoires, [...] des mains-d'œuvre bon marché, il est pensable qu'ils se battent à l'avenir pour maîtriser des informations » (Lyotard, 1979 : 7).

Au lieu de penser la société « à travers les orientations significatives régissant une communauté de culture [ou] à travers l'idéologie de légitimation associée au pouvoir et à une communauté politique » (*op. cit.*, Freitag et Bonny, 2002 : 43), nous nous appuyons maintenant sur des statistiques, des ensembles de données récupérées en temps réel, pour prendre des décisions sur le monde. Dans la modernité, non seulement les grands principes, mais aussi l'argumentation et la justification alimentaient les débats de la société. Aujourd'hui, nul besoin de se questionner, car cette société s'est redéfinie en tant que « système », et ce, par l'entremise des interactions « immédiates » de ses usagers (*Ibid.*, 2002 : 43).

Bref, le mode de reproduction décisionnel-opérationnel de Freitag nous permet d'observer dans la société postmoderne ce qui pourrait être un vide de la *praxis* humaine, une impasse dans la capacité réflexive de la société à prendre en charge son destin. Nous comprenons alors mieux pourquoi Lipovetsky aborde dans l' « ère du vide » ce qui serait peut-être la fin du politique ou une forme de société totalitaire. La société postmoderne n'a plus de projet historique mobilisateur. Cette fin du politique présente également des similitudes avec le mode de reproduction décisionnel-opérationnel de Freitag qui n'a plus de référence transcendantale : elle « rompt avec l'historicité en transformant la *praxis* politico-juridique en une opération technoscientifique libérée de la contrainte à priori du sens » (*op. cit.*, Filion, 2006 : 170). Les individus se retrouvent alors isolés dans une logique du vide, où ils ont « l'impression d'être [inutiles] socialement » (Andrieu, s. d.). Ils trouvent refuge dans ce que leur apportent les appareils technologiques sans se soucier de la collectivité et de sa destinée :

> Communiquer pour communiquer, s'exprimer sans autre but que de s'exprimer et d'être enregistré par un micropublic, le narcissisme révèle ici comme ailleurs sa connivence avec la désubstantialisation post-moderne, avec la logique du vide. (Lipovetsky, 1983 : 18)

D'ailleurs, nous pouvons faire un parallèle avec le concept d'individuation du philosophe français Bernard Stiegler. Quand Stiegler parle du *je* (individu psychique) appartenant au *nous* (individu collectif), il affirme que le « *je* se constitue en adoptant une histoire collective, dont il hérite, et dans laquelle se reconnaît une pluralité de *je* » (Stiegler, 2005 : 365). Cette pluralité de *je* se retrouve justement dans la société moderne qui est guidée par une référence transcendantale, symbolique et collective. Or, dans la société postmoderne, le *je* l'emporte sur le *nous*, car l'individu se détache de la collectivité. La montée en popularité de l'informatique, les appareils technologiques de plus en plus personnalisés et l'expansion du capitalisme semblent alors permettre à la technique de s'imposer dans la société en remplaçant toute forme

de médiations symboliques. La technique « devient alors une forme d'homogénéisation, puisque le système de la technique (re)produit *le même* aux dépens de toute extériorité et altérité » (Mondoux, 2007 : 117). Le système technique ne vise alors qu'à faire fonctionner son processus opérationnel. Les individus, qui autrefois étaient des porteurs d'outils avant l'industrialisation des machines, deviennent des ouvriers (des usagers) ou des cadres (dirigeant d'entreprises privées) servant à perpétuer ce système technique (*op. cit.*, Stiegler, 2005 : 354).

Si tel est le cas et que nous nous retrouvons dans un « système technique » qui se reproduit toujours au même (le circuit marchand des mégadonnées), cela signifie-t-il que les individus ne sont plus capables de faire valoir leur opinion en matière de vie privée en ligne ? Comment peuvent-ils réussir à s'opposer aux GAFAM qui collectent des mégadonnées si les processus opérationnels n'ont pas été conçus pour tenir compte des désirs des individus ou de la société ? Est-ce que les individus ont leur mot à dire sur ce que font les algorithmes avec leurs données ? Se retrouvent-ils en présence d'un système totalitaire ? La chercheuse belge Antoinette Rouvroy qui se spécialise dans la question des mégadonnées dirait qu' « au moins, dans un système totalitaire on sait à quoi on a affaire » (Rouvroy, 2015).

Bref, le mode de reproduction décisionnel-opérationnel de Freitag ne semble pas laisser grand espoir de changement. Cependant, ce « système technique » n'est peut-être pas aussi immuable que nous pourrions le penser. Dans cette optique, nous souhaitons aborder la notion foucaldienne de la gouvernementalité afin de voir s'il existe des possibilités de contourner cette vision qui semble être totalitaire.

2.2. Gouvernementalité et rapports de pouvoir

Le concept de la gouvernementalité a été développé à la fin des années 70 par le philosophe français Michel Foucault. La « gouvernementalité », contraction des termes « gouvernement » et « rationalité » est décrite comme une « raison gouvernementale » (Lafleur, 2017 : 142) et une forme particulière du pouvoir (Huff, 2018), c'est-à-dire une façon de gouverner par une manière de penser qui est à la fois raisonnée et logique. Il s'agit entre autres de développer les pratiques d'un gouvernement pour « assurer l'existence du corps social par l'annihilation de diverses menaces » (*op. cit.*, Lafleur, 2017 : 142). Pour bien comprendre la gouvernementalité, il suffit de revenir à la définition du pouvoir tel qu'expliqué par Foucault :

> Il ne s'agit [...] pas de repérer une instance, une [...] puissance. [...] Le pouvoir c'est des relations entre deux individus. Une relation qui est telle que l'on peut conduire la conduite d'un autre. [...] La déterminer volontairement en fonction d'un certain nombre d'objectifs qui sont les siens. [...] Le pouvoir, c'est l'exercice [du] gouvernement au sens très large. On peut gouverner une société, [...] un groupe, [...] une communauté, [...] une famille. [...] On peut déterminer sa conduite en fonction de stratégies en utilisant [des] tactiques. [...] C'est la gouvernementalité [, des] techniques qui permettent à ces relations de pouvoir de s'exercer. (Foucault, 1981)

À ce propos, Foucault a cherché par la notion de gouvernementalité à comprendre les stratégies utilisées par l'État pour gouverner à l'intérieur de la société (et non plus seulement gouverner en s'élevant au-dessus de celle-ci, comme le ferait une société féodale avec un roi) (Heyning, 1997 : 8).

Compte tenu des propos de Foucault, gouverner une société dans l'époque postmoderne peut s'avérer parfois complexe et fastidieux par sa grandeur (population grandissante, nombre de lois, etc.), mais aussi par la multitude de relations qui se crée

entre les individus. Ainsi, cet exercice peut mener ceux qui dirigent à prendre des raccourcis pour orienter la société, notamment en tentant de rassembler tous ces aspects sous une forme saisissable. Pour que le gouvernement soit à même de déterminer la conduite de sa population, il se donne alors les moyens de l'analyser en tant que « réalité naturelle et agit sur cette réalité grâce au savoir qu'il en détient » (Sibille, 2006 : 10). L'État développe des stratégies pour assurer la pérennité de ces structures hiérarchiques, mais aussi pour encadrer le développement du bien-être des individus, et ce, dans une optique de « maximisation de leur productivité » (Malette, 2006 : 80). Les instances gouvernementales utilisent comme techniques des instruments de régulation, c'est-à-dire des instruments qui, de façon générale, servent à observer et à calculer la population dans leur environnement quotidien : « ceux-ci permettent à l'État de rendre visibles et manipulables les évènements et les objets qui sont distants des centres administratifs » (*op. cit.*, Sibille, 2006 : 7).

La gouvernementalité présente également des régimes de vérité, c'est-à-dire « des types de relations qui lient les manifestations de vérité avec leurs procédures et les sujets qui en sont les opérateurs, les témoins ou éventuellement les objets » (Foucault, 1979-1980 : 98). Chaque société est caractérisée par un régime de vérité, par exemple « les types de discours qu'elle accueille et fait fonctionner comme vrais ; les mécanismes et les instances qui permettent de distinguer les énoncés vrais ou faux » (Foucault, 1977 : 158). De fait, la vérité est considérée chez Foucault comme « un ensemble d'épreuves de vérification en vertu desquelles se constituent différents modes de subjectivation des individus » (Rochon, 2014 : 78).

Or, dans le contexte actuel des mégadonnées, le régime de vérité numérique est un régime de vérité en crise selon les chercheurs Rouvroy et Stiegler. Les données extraites des individus sont décrites comme étant le réel : des données brutes, pures et vraies. Conséquemment, il n'y a pas de processus de subjectivation possible pour les

individus : « il n'y a pas d'interpellation autre que [de fausses] interpellations par des machines, par des profils, [où] la machine répond pour vous » (Rouvroy et Stiegler, 2015 : 118).

De plus, ces régimes de vérité s'insèrent aux instruments d'observation de l'État qui tendent à vouloir montrer tout ce qui doit être gouverné, car « [ce dernier] ne peut agir sur son territoire et sa population s'il n'est pas capable de les ''voir'' » (*op. cit.*, Sibille, 2006 : 8). Par exemple, le passeport est remis par le gouvernement pour ceux qui désirent traverser les frontières. Cependant, cette autorisation pour franchir le territoire ne peut être allouée si le voyageur ne spécifie pas son itinéraire aux douaniers (ville de destination, raison et durée de son séjour, etc.). Malheureusement, lire les observations effectuées sur la population se réduit généralement à simplifier leur réalité : prendre pour acquis ce que les statistiques affichent à l'égard de ce que la réalité représente elle-même pour les individus (*Ibid.*, 2006 : 8). Ainsi, le fait de traverser un territoire et de revenir sur ses pas le jour même peut s'avérer suspect pour un douanier chargé de la sécurité entre les frontières, surtout s'il a des statistiques à l'appui qui le pousse à être méfiant. Cela pourrait nécessiter plus de questions envers le voyageur ou une fouille de ces bagages. Cela conduit les individus à adopter un style de vie articulé, modulé et régulé par l'État en place. Les individus se laissent gouverner volontairement sans même réaliser ce que cela implique dans leur quotidien.

Aussi, la gouvernementalité est constituée de « rapports de pouvoir » multiples entre des dominants et des dominés (Foucault, 1976 : 121-122). Ces rapports peuvent être de nature variée (lutte, affrontement, etc.), se métamorphoser, se transformer et même s'inverser (*Ibid.*, 1976 : 121-122). Lorsqu'il est question de rapports de pouvoir chez Foucault, il y a également de la résistance, c'est-à-dire des points de fuite possibles (*Ibid.*, 1976 : 125). En effet, « toute action de pouvoir appelle, suscite, voire programme l'action qui est susceptible de lui résister. Tout flux de pouvoir appelle ce

ressac qui est une action de résistance » (Foucault, 1994 : 646). Voilà pourquoi par rapport à un pouvoir exercé par un individu ou un groupe, une résistance se manifeste de la part d'un autre individu ou d'un autre groupe afin de combattre le pouvoir mis en place (Härmälä, 2014 : 20-21). Ainsi, le circuit marchand des mégadonnées peut être interprété par des rapports de pouvoir entre les entreprises du GAFAM (dominants) et les usagers du système technique (dominés). Partant de ce fait, ces dominés pourraient chercher à résister et à créer des points de fuite à l'intérieur du rapport de pouvoir prescrit.

Par ailleurs, Foucault dit qu'une des façons d'analyser le phénomène des rapports de pouvoir est par l'entremise des discours. Selon lui, « les discours sont des éléments ou des blocs tactiques dans le champ des rapports de force » (*op. cit.*, Foucault, 1976 : 134-135). Dans une seconde préface d'*Histoire de la folie à l'âge classique*, Foucault décrit son livre non pas comme un ouvrage pédagogique, mais sous la forme d'un discours : « à la fois bataille et arme, stratégie et choc, lutte et trophée ou blessure » (Foucault, 1972). En effet, nous pourrions observer ces dualités dans une situation donnée, le discours dominant, les règles et en quoi un groupe dominé pourrait être tenté de s'approprier tel ou tel discours.

En résumé, nous avons remarqué dans les rapports de pouvoir au sens foucaldien, des points de fuites possibles qui permettent de résister et de sortir d'un rapport de pouvoir en place. Lorsque nous nous trouvons à l'extérieur de ce rapport de pouvoir, nous avons affaire à du non-rapport, où il s'avère possible d'agrandir la portée du rapport de pouvoir, c'est-à-dire l'altérer dans le but de l'améliorer. Par conséquent, des points de fuite sous forme d'extériorité permettent de créer de nouveaux rapports de pouvoir. Des individus dominés pourraient user de moyens, comme par exemple l'usage du discours, afin de sortir d'un rapport de pouvoir prescrit par des dominants, pour ensuite chercher à créer un nouveau rapport de pouvoir.

Bref, la société à mode de reproduction décisionnel-opérationnel de Freitag nous permet de conceptualiser ce qui serait peut-être la fin du politique, mais aussi la fin de la *praxis* dans un système technique qui ultimement pourrait s'avérer totalitaire s'il continue à se reproduire sans se préoccuper des individus ou de la société. Quant à la gouvernementalité de Foucault, ce concept nous apporte de nouvelles perspectives alors que les rapports de pouvoir créent des points de fuite possibles pour les individus. Ces points de fuite peuvent chercher à lutter contre des rapports de pouvoir. Par contre, ces points de fuite possibles que l'on retrouve notamment dans le discours doivent évoluer vers un discours dominant pour avoir un impact sur des rapports de pouvoir établis. Ils peuvent alors tenter de les influencer, de les altérer ou de les modifier. Ainsi, le circuit marchand des mégadonnées n'est peut-être pas aussi rigide qu'il le laisse transparaître. Il y a sans doute possibilité de venir rétablir les rapports de pouvoir en faveur des individus et de leur donner plus de contrôle pour protéger leur vie privée en ligne. Nous allons maintenant aborder la théorie de la stratégie et de la tactique de Michel De Certeau afin de nous éclairer sur les points de fuite et de résistance possibles.

2.3. Stratégie et tactique

Nous nous rapportons maintenant aux concepts de « stratégie » et « tactique ». Pour ce faire, nous nous appuyons sur la théorie des usages et des études culturelles de Michel de Certeau, historien et philosophe français du 20^{e} siècle. Dans son ouvrage *L'invention du quotidien*, l'auteur s'est attardé à la façon dont l'individu cherche à inventer son quotidien « grâce aux arts de faire, ruses subtiles, tactiques de résistance par lesquelles il détourne les objets et les codes, se réapproprie l'espace et l'usage à sa façon » (De Certeau, 1990, 4^{e} de couverture). Pour De Certeau, « le quotidien s'invente avec mille manières de braconner » (*Ibid.*, 1990 : XXXVI). Nous pourrions interpréter le fait de braconner au sens de « tricher », « voler au jeu » ou tout

simplement déjouer les règles du jeu (CNRTL, s. d.). Même si la logique opérationnelle et capitaliste s'est infiltrée dans de nombreux objets du quotidien, la manière dont les individus les manipulent, les utilisent et se les approprient n'est pas toujours prévisible :

> Dans l'espace technocratiquement bâti, écrit et fonctionnalisé où ils circulent, [les] trajectoires [des consommateurs] forment des phrases imprévisibles, des « travers » en partie illisibles. [...] Elles tracent les ruses d'intérêts autres et de désirs qui ne sont ni déterminés ni captés par les systèmes où elles se développent. (*op. cit.*, De Certeau, 1990 : XLV)

Le fait de braconner passe également par l'appropriation. L'appropriation est le « fait de s'approprier une chose, d'en faire sa propriété » (CNRTL, s. d.). En ce sens, De Certeau cherche à décrire la façon dont les usagers s'approprient les produits de consommation : « Que fabriquent-ils avec ce qu'ils absorbent, reçoivent et paient ? » (*op. cit.*, De Certeau, 1990 : 53). C'est notamment ce qui a fait l'originalité de son ouvrage à l'époque où les analyses sur les marchandises culturelles et médiatiques cherchaient à comprendre de façon statistique et rationnelle les systèmes de production et de distribution, mais : « [était] compté ce qui [était] utilisé, non les manières de l'utiliser » (*Ibid.*, 1990 : 58). C'est pourquoi De Certeau cherche à distinguer « les manières d'employer, pensées par les fabricants et celles des pratiquants, ce qu'il appelle l'appropriation » (Chavanel, s. d.).

Dans son livre, De Certeau consacre un chapitre entier intitulé « Faire avec : usages et tactiques », où il formule une distinction entre « stratégie » et « tactique ». D'un côté, nous avons la tactique qui correspond à des usages réels. Les usagers cherchent des occasions, et ce, coup par coup, pour détourner et s'approprier à leur façon les types d'opérations préétablis par des sujets de pouvoir telles une entreprise, une armée et une institution (*op. cit.*, De Certeau, 1990 : 60-61). L'une des caractéristiques importantes de la tactique, c'est l'absence d'un lieu propre. Le lieu propre est un lieu

isolable et établi par des sujets de pouvoir de manière à « gérer les relations avec une extériorité de cibles ou de menaces » (*Ibid.*, 1990 : 59). Ainsi, la tactique n'a pas besoin de délimiter un lieu pour pouvoir fonctionner. Elle « n'a pour lieu que celui de l'autre » (*Ibid.*, 1990 : 60). En effet, lorsque les sujets de pouvoir entretiennent un lieu propre, il peut y avoir une confrontation, soit un rapport de force entre des sujets de pouvoir et des usagers qui cherchent à s'approprier ou à braconner les façons de faire. La tactique cherche alors les possibilités et « [joue] dans le terrain qui lui est imposé » (*Ibid.*, 1990 : 60).

Pour mieux comprendre la tactique, De Certeau en fait la démonstration dans un environnement de travail. Dans une usine dirigée par des patrons, nous retrouvons des employés qui font « la perruque » en récupérant des restes, des biens manufacturiers non utilisés, « en vue d'un travail libre, créatif et précisément sans profit » (*Ibid.*, 1990 : 45). Nous pouvons supposer que ces restes étaient habituellement jetés par l'usine. Cependant, les employés font preuve de ruse face au champ de l'ordre établi par le lieu propre : un système économique, où des règles dans l'usine sont appliquées afin d'assurer la pérennité de la production. Les employés utilisent les retailles à leur manière, avec les machines en place, dans leur temps libre au travail. Cette utilisation peut être jugée négativement par certains patrons allant même jusqu'à accuser les employés d'être des voleurs et de « soustraire à l'usine du temps » (*Ibid.*, 1990 : 45). Pourtant, ces dirigeants oublient que les employés sont en train de créer une idée nouvelle qui n'avait pas été pensée par l'usine, soit la récupération de biens manufacturiers non utilisés pour d'autres fins que les déchets. Ces bricoleurs valorisent les produits de consommation d'une autre façon, pour des raisons parfois personnelles ou collectives (si nous pensons aux questions environnementales qui se posent actuellement).

De plus, les sujets de pouvoir entretiennent le lieu propre avec des rapports de pouvoir qui perdure dans le temps. Ils peuvent, par exemple, manipuler ou influencer

la circulation des discours. Inversement, la tactique est en mouvance. Elle mise sur une habile utilisation du temps. Elle cherche à profiter des occasions à l'intérieur du champ de l'ordre établi par les sujets de pouvoir, mais surtout des instants précis qu' « une intervention transforme en situation favorable » (*Ibid.*, 1990 : 63). La tactique n'a pas pour but de se donner un projet global. Or, elle peut chercher à affecter les rapports de pouvoir de manière à repenser le lieu propre grâce à de petites victoires.

De l'autre côté de la tactique, nous avons la stratégie qui correspond aux usages préétablis : les sujets de pouvoir (entreprises, institutions, etc.) cherchent à produire un lieu propre, à gérer les relations avec toute cible ou menace et à imposer des types d'opérations pour que les usagers puissent circuler à travers ce lieu (*Ibid.*, 1990 : 59). Le lieu propre est « ce qui maintient une extériorité à distance en vue de l'isoler, de la dompter et de la classer » (Zine, 2010 : 418). C'est en isolant un lieu propre que les stratégies sont en mesure de mieux calculer les rapports de pouvoir et faire face à toute menace. Pour créer un lieu propre, les sujets de pouvoir usent de stratégies qui cherchent à maîtriser trois types de lieux : d'abord, le lieu du pouvoir (la propriété d'un lieu propre), ensuite, des lieux de pouvoir (systèmes et discours totalisant) élaborés par ce lieu du pouvoir, enfin, des lieux physiques où les forces se répartissent au sein de ces lieux de pouvoir (*op. cit.*, De Certeau, 1990 : 62-63). Cela nous fait penser au contexte des mégadonnées. Le « système technique » peut être vu comme un système en présence de rapports de pouvoir (lieu propre), avec en son sein, un circuit marchand des mégadonnées (lieux de pouvoir), et enfin, les individus qui génèrent des traces numériques sur Internet afin d'alimenter le circuit (lieux physiques où les forces se répartissent).

Pour mettre en lumière la transition qui pourrait se produire de la tactique à la stratégie, nous pouvons nous référer à l'arrivée de la musique MP3 dans les années 90 (Mondoux, 2007 : 525-528). Après la création du format MP3 par un groupe

d'ingénieurs et l'appropriation de son usage par une communauté de *hackers*, cette nouvelle façon de lire de la musique sur un ordinateur s'est répandue dans la population et surtout auprès d'une jeune génération habile sur Internet. Le format MP3 permet notamment de stocker de la musique sur son ordinateur et de pouvoir l'échanger avec d'autres personnes. Son usage arrive donc dans l'écosystème de la musique comme une forme de détournement, déjouant la manière dont la musique avait l'habitude de circuler (ex. : achat de disques en magasin). Les individus de plus en plus portés par ce format viennent à influencer le marché économique, où le lecteur CD portatif est remplacé progressivement par le lecteur MP3 portatif. L'usage du format MP3 devient en quelque sorte la norme institutionnelle et s'impose dorénavant comme la façon actuelle de se procurer de la musique. Ainsi, l'introduction de nouvelles manières de faire dans le circuit marchand de la musique rend pratiquement caduc le format CD et amène de nouveaux rapports de pouvoir, où il est maintenant accepté et habituel de partager de la musique en format MP3.

Nous pourrions aussi faire un parallèle entre l'établissement du lieu propre de la stratégie et le mode de reproduction de la société chez Freitag. Les modes de reproduction cherchent à se reproduire dans le temps par des médiations symboliques et culturelles de manière à assurer leur continuité. C'est notamment le cas de la société moderne qui est caractérisée par l'institutionnalisation des pratiques sociales grâce à des systèmes institutionnels et juridiques. En ce sens, la composition d'une « superstructure » (*op. cit.*, Filion, 2006 : 167) d'institutions administratives se rapproche de la stratégie où le « sujet de vouloir et de pouvoir [...] est isolable » (*op. cit.*, De Certeau, 1990 : 59).

La stratégie est également présente dans la gouvernementalité de Foucault, où l'État développe des stratégies pour assurer la pérennité de ces structures hiérarchiques dans une optique de maximisation des profits. Par exemple, le système panoptique traité dans les travaux de Foucault (1975) décrivait le projet du philosophe britannique

Jeremy Bentham permettant à un seul garde de surveiller tous les prisonniers depuis son poste central. Autant dire que De Certeau a su s'inspirer des travaux de Michel Foucault et du système panoptique pour élaborer la notion de la stratégie. En effet, le système panoptique renvoie à un lieu propre qui par la mise en place de stratégies permet à la prison d'assurer sa supériorité face aux prisonniers grâce à l'aide d' « unités spatiales qui permettent de voir sans arrêt et de reconnaître aussitôt » (Foucault, 1975 : 201-202).

En plus de la stratégie et de la tactique, nous retrouvons aussi la possibilité d'un engagement de type « non-tactique ». Chez De Certeau, la tactique est présente dans toutes les pratiques du quotidien. Toutefois, les pratiques des usagers peuvent se ressembler et devenir routinières (Martínez, 2017 : 7). Ce sont des moments de similitude où les usagers ne créent pas nécessairement de résistance face aux stratégies. Ceux-ci sont même indifférents et préfèrent succomber aux pratiques mises en place par les stratégies.

En somme, la gouvernementalité de Foucault nous a permis de voir qu'il y avait des points de fuite possibles au sein des rapports de pouvoir. De Certeau nous aide à mieux observer ces rapports de pouvoir qui se créent par la production d'un lieu propre, la stratégie, et qu'il est aussi possible de braconner par l'usage de la tactique. Ainsi, le détournement s'avère une piste à explorer pour ceux qui cherchent à faire face à un système fermé et totalitaire. Les individus qui détournent les usages prescrits par les stratégies fabriquent en retour une extériorité, des tactiques, qui pourrait paver la voie à de nouveaux rapports de pouvoir et forcer l'établissement de nouvelles stratégies.

Même si le « système technique » développé par des sujets de pouvoir semble bien rigide, la notion de détournement ou de « braconnage » de De Certeau peut peut-être nous permettre d'affecter ou de modifier certains rapports de pouvoir. Sinon, nous

pourrions penser que les stratégies utilisées par les entreprises du GAFAM mèneront toujours à une forme de domination quasi totale. En effet, si la stratégie forme le tout, il n'y a plus de lieu distinct possible, c'est donc un lieu propre absolu qui prime. Par exemple, si le circuit marchand venait à devenir le système économique qui a raison d'être, il n'y aurait donc aucun moyen pour quiconque de s'opposer ou de le remettre en question. Si tel est le cas, les individus risqueraient fort bien d'être « désorbités » dans une sorte de société fourmilière :

> La généralisation et l'expansion de la rationalité technocratique ont créé, entre les mailles du système, un effritement et un pullulement de ces pratiques jadis régulées par des unités locales stables. De plus en plus, les tactiques se désorbitent. [...] De ce fait, le modèle « stratégique » mue lui aussi, comme perdu dans sa réussite : il reposait sur la définition d'un ''propre'' distinct du reste ; il devient le tout. Il se pourrait que, peu à peu, il épuise ses capacités transformatrices pour constituer seulement l'espace (aussi totalitaire que le cosmos d'antan) où s'activerait une société de type cybernétique. (*op. cit.*, De Certeau, 1990 : 65-66)

Cette société qui prend la forme d'une fourmilière s'avère préoccupante. Avons-nous affaire à ce que Freitag disait dans le mode de reproduction décisionnel-opérationnel, un monde potentiellement totalitaire où les opérations purement mathématiques ont remplacé toute forme de médiations transcendantales ?

Pour aborder cette situation, nous allons recueillir les propos d'individus issus d'une organisation de sensibilisation qui cherche à lutter contre des sujets de pouvoir dans le contexte actuel des mégadonnées. Pour des organisations qui cherchent à sensibiliser leur communauté au sujet de la vie privée en ligne, le défi est de taille. Pour s'opposer aux GAFAM, elles doivent se heurter à plusieurs obstacles : le vide de la *praxis*, la montée en popularité de l'informatique personnalisée, la suprématie de la technique et l'expansion du capitalisme. Les entreprises du GAFAM usent de stratégies pour assurer la pérennité de leur lieu propre, le circuit marchand des mégadonnées. Ce qui leur assure un rapport de pouvoir dominant face aux usagers.

Par conséquent, les organisations de sensibilisation doivent déployer des tactiques afin de redéfinir le rapport de pouvoir en place et chercher à créer de nouveaux rapports de pouvoir. Ces tactiques doivent également être institutionnalisées et se transformer en stratégie pour qu'elles puissent perdurer dans le temps.

2.4. Questions de recherche

Il existe plusieurs organismes de sensibilisation dans le monde qui s'intéressent aux enjeux numériques et qui sont critiques des entreprises du GAFAM : *Electronic Frontier Foundation*, *The Tor Projet*, *Big Brother Watch*, etc. Au Canada, nous retrouvons OpenMedia à Vancouver, un organisme sans but lucratif (OSBL) de défense des droits des consommateurs fondés en 2008. L'organisme a notamment créé une pétition *Protect Our Privacy* afin de demander aux gouvernements de mettre en place des mesures pour protéger la vie privée des citoyens canadiens face à l'intrusion d'entités gouvernementales (OpenMedia, 2013). À l'est du pays et plus près de chez nous, nous retrouvons Crypto.Québec. L'OSBL a été fondé en 2015 et cherche à sensibiliser la population aux enjeux touchant la sécurité informatique, la vie privée et la technologie de l'information.

Il nous apparaît pertinent de nous intéresser aux propos de Crypto.Québec, afin de voir s'il existe des moyens à notre échelle pour s'opposer aux GAFAM dans le contexte des mégadonnées. D'un côté, nous avons des usagers qui accèdent à des plateformes tout en banalisant la lecture des conditions d'utilisation et qui cherchent à protéger leur vie privée par l'usage de solutions individuelles et techniques. De l'autre côté, nous avons des entreprises privées qui, par la mise en place d'un lieu propre, cherchent à camoufler les enjeux entourant la captation des données de leurs usagers. Au centre, il semble y avoir Crypto.Québec qui tente de vulgariser l'information numérique et les enjeux associés pour le bien de sa communauté.

Suivant notre question générale de recherche – **dans un tel contexte, comment Crypto.Québec peut-il affecter, modifier ou détourner les rapports de pouvoir du circuit marchand des mégadonnées induits par les GAFAM ?** –, notre réflexion s'articulera autour des questions suivantes :

1. Les pratiques mises de l'avant par Crypto.Québec s'inscrivent-elles comme tactique au sens indiqué par De Certeau ? Nous avançons ici une première hypothèse selon laquelle, comme nous l'avons vu avec dans la stratégie et la tactique de De Certeau, il existe des points de fuite et des occasions pour l'organisme de s'approprier les « manières de faire ».

2. Crypto.Québec est-il en voie de devenir stratégique au sens indiqué par De Certeau ? Si tel est le cas, les stratégies utilisées par l'organisme peuvent-elles influencer les rapports de pouvoir du circuit marchand des mégadonnées ? Ce qui nous amène à notre seconde hypothèse, selon laquelle dans le contexte postmoderne (mode de reproduction décisionnel-opérationnel), nous croyons qu'il est encore possible pour un organisme d'utiliser des tactiques de façon stratégique pour venir rééquilibrer les rapports de force induits par les GAFAM. Nous pouvons supposer que ces tactiques doivent être institutionnalisées afin d'avoir un lieu propre réfléchi pour le bien de la communauté (et opposé à la logique économique et capitaliste). Nous pouvons penser également que ces stratégies ont un impact sur les rapports de pouvoir du circuit marchand, de manière à altérer ou modifier le lieu propre prescrit par les GAFAM.

2.5. Pertinence et originalité

2.5.1.Pertinence sociale

Pour la pertinence sociale, nous pensons que notre recherche entraînera une prise de conscience dans la navigation sur le Web. Dans le contexte actuel, les usagers doivent dans la majeure partie des cas céder leurs données pour accéder et profiter gratuitement des services des sites Web ou des applications (particulièrement les médias socionumériques). En ce sens, si l'accès semble être gratuit, c'est que nous en sommes le produit (La Quadrature du Net, 2016). Bien que la plupart des services demandent aux usagers de lire et d'accepter des conditions d'utilisation, ces derniers n'ont pas toujours conscience de l'étendue des données récoltées et des risques potentiels (par exemple, Facebook stipule dans ces conditions d'utilisation qu'ils ne peuvent garantir que leurs produits seront « toujours sûrs, sans risques ») (Facebook, 2018). En mars 2018, l'affaire de la société d'analyse Cambridge Analytica qui a pris les données de plus 50 000 millions d'usagers de Facebook sans leur consentement afin de faire du ciblage publicitaire lors de la campagne présidentielle aux États-Unis (Giles, 2018), démontre l'urgence d'agir pour mieux comprendre les mégadonnées. Dans ce scandale, des usagers ayant utilisé une application de tests psychologiques sur Facebook a permis de récolter des données sur un nombre encore plus élevé de données (non seulement les données du sondage, mais également, les données des amis des usagers sondés). Il devient alors nécessaire pour un usager de connaître les données qu'il peut transmettre sur Internet, mais aussi d'explorer les possibilités de naviguer sans avoir à céder ses données ou en limitant leur récolte. Cette recherche pourrait donc mener vers de nouvelles pratiques et des retombées positives pour les usagers soucieux de leur présence numérique.

2.5.2.Pertinence scientifique

Pour la pertinence scientifique, nous croyons que notre recherche fera naître des connaissances nouvelles sur le phénomène des mégadonnées, mais aussi sur la théorie de la stratégie et de la tactique. De fait, nous pensons qu'il s'avère pertinent d'analyser une organisation qui traite des enjeux de surveillance et d'identification au Québec. Nous pourrions étudier la façon dont elle utilise son discours pour vulgariser l'information numérique auprès de sa communauté, comment elle décrit son terrain de jeu pour interagir avec les usagers et les élites de la société (politique, médias, etc.) et où l'organisation se situe dans la théorie de la stratégie et de la tactique. Cela nous permettrait également de réactualiser la théorie de De Certeau dans de nouvelles avenues de recherche.

CHAPITRE 3

MÉTHODOLOGIE QUALITATIVE

Nous avons cherché à répondre à nos questions et nos hypothèses spécifiques de recherche par l'entremise d'une stratégie de *recherche qualitative*. De manière inductive, nous avons tenté de « déterminer les principaux éléments à mettre en relation pour produire une représentation cohérente, un modèle, qui puisse servir à appréhender telle ou telle situation » (Mongeau, 2008 : 30). Nous avons opté également pour une « observation flexible de la réalité » où nous nous sommes laissé guider par notre intuition et notre jugement (Lamoureux, 2000 : 39), tout en appliquant de façon rigoureuse et critique des stratégies d'analyse.

3.1. Choix de l'objet de recherche

3.1.1.Crypto.Québec

Pour ce faire, nous avions l'intention d'analyser le discours de Crypto.Québec, un organisme sans but lucratif (OSBL) ayant pour mission de devenir « la référence au Québec en termes d'information vulgarisée et factuelle sur les enjeux de sécurité informatique, géopolitique, vie privée, technologie de l'information et renseignement » (Crypto.Québec, 2018). Fondé en juillet 2015 à Montréal, l'OSBL échange avec sa communauté à travers différentes plateformes numériques telles que

leur site Web, leurs médias socionumériques et de la baladodiffusion (avec des dizaines de milliers d'auditeurs francophones revendiqués) (*Ibid.*, 2018). Par l'entremise de plusieurs services (conférence, formation, service-conseil aux cabinets professionnels, entrevue média), Crypto.Québec « s'engage [...] à soutenir l'émancipation et l'avancement des libertés individuelles et collectives québécoises » (*Ibid.*, 2018). L'équipe de Crypto.Québec est composée de six membres, d'un conseil d'administration, d'un conseil exécutif ainsi que des bénévoles qui les accompagnent. La plupart de ses représentants s'intéressent ou travaillent de près dans l'univers du numérique. Par exemple, la directrice des opérations, Geneviève Lajeunesse, possède plus de 10 années d'expérience dans le domaine des médias numériques et travaille comme productrice et analyste stratège pour un studio de jeu vidéo à Montréal. Enfin, l'organisme alimente régulièrement un blogue sur leur site Web. Plus de la moitié des articles du blogue sert à la promotion de leur émission hebdomadaire en baladodiffusion, intitulée *Les chiens de garde.* Nous avons compté plus de 80 émissions qui traitaient des « enjeux de sécurité informatique, de vie privée, de surveillance et tout ce qui s'y rattache » (*Les chiens de garde*, s. d.). Les autres billets du blogue regroupaient des annonces de l'équipe, des articles sur l'actualité ainsi que des entrevues accordées dans les médias.

Nous avons choisi cette organisation pour deux principales raisons. Premièrement, elle se situe au cœur même des débats contemporains en ce qui a trait aux enjeux sur la sécurité des données informatiques. Comme nos intérêts de recherche, les mégadonnées, l'identification et la surveillance sont traités régulièrement par l'organisme, il semblait judicieux de les consulter. Deuxièmement, l'OSBL communique par le biais de leurs plateformes et de leurs services, avec différents publics pour faire valoir leurs intérêts. Il cherche à intervenir auprès de la communauté des usagers du Québec en offrant de l'information hebdomadaire, des formations et des ateliers. Toutefois, il est également reconnu pour son expertise et est invité régulièrement par des médias afin de commenter les nouvelles de l'actualité

dans le domaine des NTIC. Cela permet à Crypto.Québec de partager son point de vue et d'influencer à plus grande échelle la population. Nous y avons vu un énorme potentiel pour approfondir les théories abordées précédemment en puisant dans le contenu du discours de l'organisme.

3.1.2.Sélection du corpus discursif

Avant de commencer la sélection du corpus, nous avons effectué une étude préliminaire. Nous avons regardé notamment l'ensemble des moyens de communication utilisés par l'organisme (site Web, blogue, baladodiffusion, médias socionumériques), les différentes interventions de leurs membres dans les médias, mais aussi leur présence à des évènements et à des conférences. Nous avons notamment constaté que Crypto.Québec publiait régulièrement leurs interventions dans les médias sur leurs pages Facebook et Twitter alors qu'elles n'étaient pas nécessairement traitées dans leurs émissions de baladodiffusion. Également, nous avons remarqué que les balados offraient un contenu plus long et flexible dans la variété des sujets traités alors que les interventions dans les médias étaient plus concises, limitées et basées en fonction de l'actualité médiatique. Ainsi, cette étape nous a permis de rassembler les principaux canaux d'information et de nous familiariser avec le contenu produit par l'organisme. Également, nous avons pu entrevoir le point de vue de leur public et constater l'ampleur de leurs différentes interventions. Étant donné que nous cherchions à étudier le discours de Crypto.Québec dans son ensemble, nous avons rassemblé tous les documents que nous pouvions récolter à leur sujet sur une période approximative d'un an pour avoir une meilleure représentation de leur réalité. Ainsi, nous croyons que peu de documents ont été écartés de notre recueil.

La sélection du corpus a été effectuée par l'entremise du site Web et des médias socionumériques de Crypto.Québec, mais aussi avec des recherches par mots-clés de l'organisme sur les sites Eureka et Google Actualités. Les critères de sélection des documents étaient les suivants : 1) être créé par les membres de Crypto.Québec ou avec leur participation ; 2) être un document médiatique (écrit ou parlé) ; 3) avoir un contenu qui se rapproche de nos intérêts de recherche (nous avons écarté des sujets intéressants, mais qui s'éloignaient de nos intérêts, par exemple : la cybermonnaie, la biométrie, etc.) ; 4) avoir été créés entre mars 2017 et avril 2018.

Les documents sélectionnés ont fait l'objet d'une vérification. Nous avons lu, écouté, regardé chacun de ceux-ci afin de nous assurer qu'ils répondaient à nos critères de sélection. Au total, nous avons retenu 43 documents, dont 15 émissions en baladodiffusion, 6 publications sur leur site Web, 3 pages Web sur des sites partenaires, 2 pages d'évènements sur Facebook et, enfin, 17 interventions publiques sous des formes variées dans les médias (journal, radio, télévision). La liste complète des documents se trouve en Annexe 2 et est détaillée par titre, type de communication, source, support, locuteur et date de diffusion.

3.2. Analyse critique du discours

3.2.1.Les principes fondamentaux de l'ACD

Pour analyser l'ensemble des documents sélectionnés, nous nous sommes inspiré des théories et des méthodes qui s'inscrivent dans le courant de l'analyse critique du discours (ACD) (*Critical Discourse Analysis*). Ce courant est apparu au début des années 90 après qu'un groupe de chercheurs issus de domaines variés (rhétorique, linguistique textuelle, anthropologie, philosophie, sociologie, pragmatisme, etc.) se soient réunis pour discuter de l'analyse du discours dans leurs travaux de recherche

(Teun A. Van Dijk, Norman Fairclough, Gunther Kress, Theo Van Leeuwen et Ruth Wodak) (Wodak et Meyer, 2009 : 1-2). L'ACD se définit comme une forme d'analyse de discours qui cherche à révéler les relations de pouvoir, de domination et d'exclusion que l'on retrouve au sein d'une société qui sont exprimées et reproduites dans les textes et paroles des groupes et institutions influents (Van Dijk, 2008 : 84). En d'autres mots, nous nous sommes intéressé particulièrement à la façon dont les rapports de pouvoir et l'inégalité sociale sont reproduits ou débattus par les groupes sociaux, et ce, par l'entremise de leur discours (Van Dijk, 1995 : 18). De fait, l'un des principaux objectifs de l'ACD est de prendre conscience de la domination exercée par certaines personnes sur d'autres personnes par le discours (Fairclough, 1989 : 3). Lorsque nous pouvons identifier l'existence de certaines inégalités sociales, il semble alors plus facile de s'y attarder pour chercher à s'en libérer. C'est pourquoi l'un des objectifs de l'ACD est non seulement de décrire ou d'explorer une réalité, mais surtout de révéler, dévoiler, divulguer ce qui est dissimulé dans le discours des élites du pouvoir (*op. cit.*, Van Dijk, 1995 : 18).

De plus, quatre éléments peuvent illustrer certains des principes fondamentaux de l'ACD : le discours, la critique, l'idéologie et le pouvoir (*op. cit.*, Wodak et Meyer, 2009 : 4). Premièrement, le discours est vu comme une forme de pratique sociale. Il s'agit bien plus qu'un message produit (à l'oral ou à l'écrit) par un émetteur (locuteur) et adressé à un destinateur (interlocuteur). Cette forme « implique une relation dialectique entre un évènement discursif particulier et la ou les situations, institutions et structures sociales qui l'encadrent[23] » (*Ibid.*, 2009 : 5). Nous pouvons dire que le discours se construit de manière bilatérale, car il est constitué par ce qui l'entoure, mais il est également constituant des relations sociales. Deuxièmement, l'élément « critique » pour les chercheurs de l'ACD est le fait d'examiner, de commenter et de juger un discours afin de produire des connaissances nouvelles.

[23] Traduction libre

Nous pouvons ainsi les partager et aider d'autres personnes à prendre conscience d'une situation donnée aux prises avec certaines formes de domination, de manière à permettre leur émancipation (*Ibid.*, 2009 : 7). Troisièmement, l'ACD décrit les idéologies comme étant « le fondement des représentations sociales partagées par un groupe[24] » (Van Dijk, 2006). Elles sont « des complexes schématiquement organisés de représentations et d'attitudes à l'égard de certains aspects du monde social, par exemple, les représentations [...] qu'ont les personnes blanches des personnes noires[25] » (Van Dijk, 1993 : 258 ; cité dans Van Dijk, 2009 : 9). Elles sont des « représentations d'aspects du monde qui contribuent à établir et maintenir des relations de pouvoir, de domination et d'exploitation[26] » (Fairclough, 2003 : 218, cité dans *Ibid.*, 2009 : 9). Les idéologies s'insèrent si bien dans la vie quotidienne qu'elles semblent souvent faire partie des croyances et des opinions évidentes de la société (Van Dijk, 2006 : 177), ce qui les rend plus difficiles à remettre en question ou à critiquer.

Enfin, les rapports de pouvoir apparaissent comme un concept central pour les chercheurs de l'ACD, notamment dans le discours utilisé par ceux qui possèdent une certaine autorité et qui sont responsables des inégalités sociales (*op. cit.*, Van Dijk, 2009 : 9). À noter que le pouvoir ne découle pas nécessairement du discours. Ce sont les personnes investies d'un pouvoir qui donnent une force au discours et le rendent puissant. De plus, il est souvent possible de percevoir dans les discours, de par sa nature relationnelle, « des lieux de lutte [...] [,] des traces de discours et d'idéologies divergentes qui luttent pour dominer[27] » (*Ibid.*, 2009 : 10).

[24] Traduction libre
[25] Traduction libre
[26] Traduction libre
[27] Traduction libre

3.2.2.L'analyse de discours idéologique

Dans le cadre tridimensionnel de l'ACD, conçue par l'un des fondateurs du courant, le chercheur anglais Norman Fairclough, nous pouvons mener une analyse du discours en trois dimensions : 1) le texte (l'objet d'analyse : textuel, verbal ou visuel), 2) la pratique discursive (les processus par lesquels l'objet d'analyse est produit et interprété par des personnes) et 3) le contexte socioculturel qui régit ces processus (Fairclough, 1995 : 96 ; Janks, 1997). La troisième dimension nous a attiré particulièrement, car nous nous intéressions aux questions de pouvoir et d'idéologie. Nous désirions analyser « différents niveaux d'organisation sociale – le contexte de la situation, le contexte institutionnel et le contexte sociétal plus large ou ''contexte de la culture''[28] » (Fairclough, 1995 : 95).

Bien que nous nous sommes attardé à chacune de ces dimensions de l'ACD, nous n'avions pas pour objectif de comprendre le fonctionnement du langage en tant que tel ni les aspects formels du texte (Quivy et Campenhoudt, 1988 : 216). Bien que les recherches en sémiotique et linguistique puissent s'avérer intéressantes pour certains auteurs de l'ACD, avec une méconnaissance en la matière et pour des contraintes de temps qui nécessiteraient l'apprentissage de ces théories dans le cadre de cette recherche, nous avons laissé le soin à des chercheurs plus expérimentés que nous de poursuivre les recherches en ce sens. Nous souhaitions plutôt traiter de manière méthodique les informations qui se dégagent du corpus sélectionné et, plus particulièrement, décrire et montrer ce qui est dissimulé dans le discours en termes de rapports de pouvoir. Pour ce faire, notre démarche s'est inspirée des travaux du linguiste néerlandais Teun A. Van Dijk (2000) sur une version de l'ACD, l'analyse de discours idéologique. Le cadre proposé par Van Dijk a pour but de favoriser la compréhension de la nature et des fondements des idéologies dans la société.

[28] Traduction libre

Rappelons que l'idéologie est décrite « comme une forme de pratique sociale, et plus spécifiquement comme les croyances fondamentales qui sous-tendent les représentations sociales d'un groupe social[29] » (Van Dijk, 2000 : 16). En ce sens, Van Dijk propose un schéma pour organiser les idéologies. Celui-ci est composé de six catégories qui représentent les dimensions principales d'un groupe social :

- « Critères d'appartenance : À qui appartiennent les individus d'un groupe social (ou n'appartiennent pas) ?
- Activités typiques : Que font-ils ?
- Objectifs généraux : Que veulent-ils ? Pourquoi le font-ils ?
- Normes et valeurs : Qu'est-ce qui est bon ou mauvais pour eux ?
- Position : Quelles sont leurs relations avec les autres ?
- Ressources : Qui a accès aux ressources de leur groupe ?[30] » (Van Dijk, 2000 : 17).

Cette liste de questions permet de mieux décrire ce que peut ressentir une personne qui fait partie d'un groupe, notamment son sentiment d'appartenance à une identité sociale (Van Dijk, 2000 : 18). Elle permet également d'apercevoir la place et la position qu'elle occupe dans le groupe social.

3.3. Analyse du discours de Crypto.Québec

3.3.1. Grille d'analyse et encodage

En nous inspirant de la théorie de De Certeau et en nous basant sur les théories de l'ACD et le cadre de l'analyse de discours idéologique de Van Dijk, nous avons préparé une grille d'analyse pour nous aider à traiter le discours de Crypto.Québec.

[29] Traduction libre
[30] Traduction libre

La préparation de cette grille s'est effectuée en deux temps. Premièrement, nous avons élaboré une grille d'analyse par le biais de thèmes et de série de questions (voir tableau 3.1 à la page suivante). À la manière d'un entonnoir, nous avons structuré et opérationnalisé notre grille en débutant par notre concept principal « détournement » découlant de nos questions de recherche (Lamoureux, 2000 : 116-117). Nous avons ensuite dégagé quatre dimensions/catégories pouvant étudier notre concept principal : tactique, stratégie, tactique à stratégie et protagoniste. Puis, nous avons cherché à circonscrire davantage les dimensions par des sous-catégories, car elles représentaient selon nous différents aspects des dimensions. Ensuite, nous avons formulé des questions pour chacune des catégories ou sous-catégories à titre indicatif pour nous guider dans la collecte des données. Pour cette étape, nous nous sommes inspiré des questions du schéma social sur les idéologies de Van Dijk (2000).

Avec cette grille, nous souhaitions comprendre les tactiques et stratégies employées par l'organisme pour faire face aux entreprises de plateformes numériques. Pour la tactique, nous avons analysé leurs moyens de communication, leurs pratiques et leurs services (sous-thèmes). Pour ce qui est de la stratégie, nous avons analysé les différents lieux d'action qu'ils utilisent pour interagir avec d'autres organisations. Nous souhaitions également voir ce qu'ils entendaient par « tactique » et « stratégie » et s'ils avaient des exemples pour mettre en relation ces termes avec leurs expériences. Puis, nous voulions connaître les différents protagonistes qui les entouraient (ex. : *hackers*[31], citoyens numériques[32], etc.) dans le contexte actuel et où ils se situaient dans un rapport de pouvoir (ex. : dominé/dominant). Ensuite, nous

[31] Comme la traduction « pirate informatique » nous apparaît péjorative, nous préférons le terme anglais *hacker* (communément connu comme « bidouilleur » en français et « gosseux » en québécois) pour décrire ceux qui ont une « passion immodérée pour tout ce qui a trait à l'informatique » (OQLF, 2006).

[32] La citoyenneté numérique peut avoir de multiples significations. Nous nous appuyons sur une définition souple des chercheurs français Greffet et Wojcik, où il s'agit d'une « relation à l'ordre politique au sens large, relation médiatisée par les technologies numériques, et dont les formes, les lieux et les enjeux varient dans le temps et l'espace » (Greffet et Wojcik, 2014 : 152).

voulions connaître leur point de vue à propos des relations avec leurs alliés et leurs adversaires, mais aussi la perception de ces derniers sur les tactiques et stratégies employées par l'organisme. Notre grille d'analyse était la suivante :

Tableau 3.1 – Grille d'analyse

Concept	Thèmes	Sous-thèmes	Questions
Détourne-ment	Tactique	Moyens (A)[33]	Que font-ils ? Qui a accès aux ressources de leur groupe ? Quels sont leurs moyens de communication (pratiques, activités, services) ? Quelles sont leurs pratiques qu'ils utilisent en matière de protection de la confidentialité et de la surveillance ? Pourquoi utilisent-ils ces pratiques ?
		Conseils (B)	Quoi répondre à une personne désirant se protéger en ligne ?
		Défis (C)	Qu'est-ce qui est bon ou mauvais pour eux ? Quelles sont les limites de leurs pratiques ? Se sentent-ils écoutés ? Quels sont les défis qu'ils rencontrent ?
	Stratégie	Moyens (D)	Que font-ils ? Qui a accès aux ressources de leur groupe ? Comment s'y prennent-ils pour développer et pérenniser leurs pratiques ? Dans leurs pratiques, quel est leur lieu d'action (dans la mesure où ils peuvent entrer en discussion avec un pouvoir de par leur espace, par exemple, un quartier général) ? Ont-ils un bulletin de liaison (ex. : calendrier des activités) ?
		Défis (E)	Qu'est-ce qui est bon ou mauvais pour eux ? Quelles sont les limites de ces pratiques ?
	Tactique à stratégie		Est-ce qu'ils misent sur des pratiques à court terme ou des pratiques à long terme ou les

[33] Une lettre a été attribuée à chacun des sous-thèmes afin de faciliter la classification des données. Par exemple, suivant le corpus des documents sélectionnés (voir Annexe 2), une citation provenant de la première source du corpus, l'émission en baladodiffusion « 40 : Questions du public, les IMSI… », répondant à l'une des questions du sous-thème « Moyens » dans le thème « Tactique » est identifiée par la nomenclature suivante : A1.

	(F)		deux ? Est-ce qu'il y a des pratiques à court terme qui mènent à des pratiques à long terme ?
	Protagoni-ste	Définition (G)	Qui est concerné par les enjeux d'identification et de surveillance (*hackers*, citoyens numériques, gouvernement, etc.) ?
		Rapports de pouvoir (H)	Quel rapport de pouvoir observent-ils en termes de lutte, d'affrontement, de résistance entre les protagonistes (par exemple, les dominants versus les dominés) ?
		Alliés (I)	Qui sont leurs alliés ? Quels sont leurs rapports avec les alliés ?
		Adversaires (J)	Qui sont leurs adversaires ? Quels sont leurs rapports avec les adversaires ?

3.3.2.Personnalisation et utilisation d'un document inspiré du logiciel TAMS Analyser

Dans le cadre du recensement des documents pour notre corpus, nous avons préparé un document composé de différentes sources de l'organisme Crypto.Québec. Il nous apparaissait plus adéquat de réunir en seul endroit toutes nos annotations. Nous avons d'abord testé TAMS Analyser, un logiciel américain d'encodage et d'extraction, pour voir s'il répondait à nos besoins. Pour deux raisons, nous avons vite abandonné son utilisation. Premièrement, le logiciel n'était pas adapté à la dernière version du système d'exploitation de notre ordinateur Mac, ce qui laissait à désirer pour la sécurité de nos données. Deuxièmement, des fonctionnalités non intuitives nous faisaient craindre la perte de nos données. Plus précisément, lors des sauvegardes, le logiciel créait des fichiers que nous devions récupérer à l'extérieur de la plateforme (dans des sous-dossiers), ce qui nous amenait parfois à égarer des annotations.

Néanmoins, nous nous sommes inspiré du style d'encodage du logiciel TAMS Analyser pour bonifier notre document actuel. D'abord, nous avons rassemblé dans un seul document tout le corpus sous forme textuelle (baladodiffusion, entrevue télé, article, etc.). Ensuite, nous avons créé différents codes associés aux thèmes et sous-thèmes de notre grille d'analyse. Puis, nous avons annoté chacune des sources à l'aide de notre encodage. Par exemple, nous remarquons dans l'extrait ci-dessous que {Tacti>Defi} est utilisé pour le sous-thème « défi » dans la thématique « tactique », ainsi que {Tacti>Strat} pour le thème « tactique à stratégie ».

> {Tacti>Defi} La sécurité absolue ça n'existe pas vraiment puis même quand ça existe c'est hors de portée malheureusement {/Tacti>Defi} [...] Devrions-nous avoir peur ? Moi {Tacti>Strat} je dirais si la peur peut générer en quelque sorte que les gens restent à l'affût se tiennent informer puis qu'ils fassent une certaine curation à leur cercle de confiance, tant mieux ! Mais c'est vraiment ça la solution. C'est pas une question il faut avoir peur il faut juste rester critique et à l'affût {/Tacti>Strat}.

Par une recherche par mots-clés des codes, nous avons ensuite rassemblé les différentes données sous chaque question dans un tableau à cet effet. Ici-bas un extrait du tableau à propos du code {Tacti>Moy} :

Tableau 3.2 – Exemple de collecte de données – Document A

#	Code	Données	Titre du document	Type de communication	Source	Support	Locuteur	Date de diffusion
1	{Tacti> Moy}	Reportage de [...] Geneviève qui avait réussi à s'introduire dans l'appareil de Marie-Ève	40 : Questions du public, les IMSI catchers de GRC et la National Geospatial-Intelligence Agency	Émission de baladodiffusion	*Les chiens de garde* (Crypto. Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu, Sophie Thériault	2017-03-22
2	{Tacti> Moy}	Jean-Philippe t'es allé au Web à Québec la semaine dernière. Oui, moi et Luc on avait une conférence sur le *dark web*, la plus grosse conférence numérique francophone en Amérique du Nord, la seule [...] on a su démystifier le *darknet* Ce matin j'ai passé à Paul Arcand pour parler du *darknet* justement On offre des services puis des formations aux journalistes pour sécuriser les données [...] Patrick Lagacé et autres journalistes pourraient être intéressés à pu se faire épier par le SPVM ou autre service de police ou de renseignement ou du crime organisé ou peu importe [...] y'a des moyens contre ça, on les a	43 : Une sécurité des données déficiente au SPVM, ShadowBrokers qui publie des outils de la NSA et le démantèlement du botnet Kelihos	Émission de baladodiffusion	*Les chiens de garde* (Crypto. Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Jean-Philippe Décarie-Mathieu	2017-04-12

4	{Tacti> Moy}	Présentation sur le téléphone mobile Montreal All Girl Crypto.Brunch le 18 juin [...] vous pouvez vous inscrire sous un pseudonyme [...] ça va être un matin dans lequel vous allez pouvoir passer de station en station avec des formateurs selon vos intérêts puis vos besoins par rapport au chiffrement puis à la sécurité puis autour d'un petit smoothie on va être capable d'améliorer chacun notre posture	49 : Les politiques de modération de Facebook, la surveillance des militants à Standing Rock et l'origine de Shadow Brokers	Émission de baladodiffusion	*Les chiens de garde* (Crypto. Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Sophie Thériault	2017-05-31
6	{Tacti> Moy}	On connait le principe c'est une revue de presse Crypto.Québec aux chiens de garde Merci à tous ceux qui sont venus au Crypto.Brunch la semaine dernière [...] c'est une belle réussite de notre côté [...] autant de votre côté si je me fis au *feedback* qu'on a eu [...] c'était à l'UQAM [...] la salle était pleine 50-60 personnes facile [...] pour une journée [...] beaucoup de questions [...] pertinentes	53 : Petya, la Chambre des communes anglaise compromise et un porte-avion roulant sous Windows XP	Émission de baladodiffusion	*Les chiens de garde* (Crypto. Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu	2017-06-28
7	{Tacti> Moy}	C'est l'été on se promène beaucoup [...] de façon générale en tant qu'équipe. Invitez-nous par chez vous si vous avez du temps dans une fin de semaine [...] [,] de l'espace pour accueillir des gens pour parler de crypto [...] [,] un petit groupe qui se réunit autour des enjeux pas besoin d'être autour de la vie privée ça peut être un groupe d'activistes ou peu importe on est intéressé à vous rencontrer	54 : Les PMEs et les attaques informatiques, wangiri et un coup de filet de la police sur le darknet	Émission de baladodiffusion	*Les chiens de garde* (Crypto. Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu, Anne-Sophie Letellier	2017-07-05

CHAPITRE 4

RÉSULTATS

Pour la réduction des données, nous avons encodé chacun des extraits par rapport aux thèmes de notre grille d'analyse et nous avons terminé l'exercice lorsque le principe de saturation est apparu, c'est-à-dire lorsqu'il n'y avait plus rien de nouveau qui émergeait en termes de contenu (Mongeau, 2008 : 106). Dans ce chapitre, nous présentons les résultats de cette réduction pour permettre au lecteur « de prendre directement connaissance de nos résultats » (*Ibid.*, 2008 : 111). Pour ce faire, nous cherchons à montrer « la réalité observée telle qu'elle est vécue par les acteurs » (*op. cit.*, Lamoureux, 2000 : 206). Ainsi, nous avons sélectionné quelques extraits qui permettent de représenter au mieux le discours de Crypto.Québec.

4.1. Changer les habitudes de la population

Crypto.Québec se décrit comme un organisme qui cherche à sensibiliser la population, mais aussi les entreprises et les institutions, aux enjeux de sécurité informatique, de surveillance et de protection de la vie privée en ligne. L'organisme le fait en accord avec ses valeurs, soit de soutenir « l'émancipation et l'avancement des libertés individuelles et collectives » (D17[34])[35]. Pour arriver à ses fins, l'organisme utilise plusieurs moyens de communication pour sensibiliser la

[34] La nomenclature de cette référence (et de celles à venir) est précisée dans une note en page 55.
[35] Comme le rappelle le slogan « En toute liberté » mis de l'avant sur le site Web de Crypto.Québec.

population, notamment leur émission en baladodiffusion *Les chiens de garde*. Il s'agit d'un moyen privilégié par l'organisme pour communiquer sur une base régulière (presque hebdomadaire) avec ses abonnés. Le but de l'émission est double. Elle cherche à la fois à vulgariser et à démystifier l'actualité, mais aussi à fournir des conseils pour améliorer sa présence numérique : « On vise à vous permettre d'adopter des meilleures habitudes, puis peut-être manquer un peu de sommeil parce que parfois les nouvelles sont un peu inquiétantes » (A12). À la manière d'une revue de presse, l'émission aborde l'actualité sous différents angles (*hacking*, conseils, surveillance, vie privée, sécurité, politique, etc.) et traite de récentes nouvelles de l'équipe avec la rubrique « annonces » (intervention dans les médias, participation à une conférence, etc.) (voir Annexe 3). Au départ, le groupe ne pensait pas être en mesure de réunir suffisamment de contenu pour leur balado. L'actualité concernant le numérique, qui ne cesse d'augmenter, les a finalement convaincus du contraire : « Est-ce qu'y a assez de contenu pour une émission hebdomadaire ? [...] En masse, en masse » (F8).

Crypto.Québec est aussi invité à commenter l'actualité numérique[36] dans les médias de notoriété au Québec (Ici Radio-Canada, La Presse, 98,5 FM, etc.) (G1, G2, G9), ce qui leur permet de rejoindre un public plus large. Pour les médias, l'organisme est une référence dans son domaine d'expertise : « Un média nommé Crypto.Québec travaille à offrir aux citoyens des clés pour éviter que leur vie privée soit, en ligne, sans filtre » (D32). L'effet de levier entre en jeu, car les interventions publiques permettent d'accueillir de nouveaux auditeurs à leur émission : « Pour ceux qui nous écoutent pour la première fois [...] on a fait plein d'entrevues cette semaine, c'est assez dur de savoir d'où vous venez » (A14). Bien que le groupe soit amené à

[36] Les principaux sujets d'actualité pour lesquels des membres de l'organisme ont été invités à commenter durant la période étudiée (mars 2017 à avril 2018) sont notamment : le rançongiciel WannaCry (juin 2017), les failles informatiques Spectre et Meltdown (janvier 2018), et le scandale de Facebook-Cambridge Analytica (mars 2018). Spectre et Meltdown permettaient aux malfaiteurs d'accéder en quelque sorte « au noyau d'un système d'exploitation informatique, par exemple des mots de passe » (La Presse, 2018).

discuter des évènements qui occupent la scène médiatique, il arrive parfois que des sujets qui s'avèrent intéressants pour l'organisme n'occupent que très peu la place publique. Par exemple, dans le cas de la *Journée de la protection des données*, seul un média a approché l'organisme (la chaîne de télévision V pour l'émission *NVL*), et ce, pour une entrevue qui a été diffusée à l'extérieur des heures de grande écoute : « J'ai eu droit à un topo d'une minute sur V le samedi soir à 23 h 50 » (A11).

En considérant leurs émissions, leurs interventions publiques et les autres documents du corpus (publications sur leur site et les sites partenaires), nous pouvons faire ressortir deux moyens employés par Crypto.Québec pour permettre à la communauté d'adopter de nouvelles habitudes en ligne : des conseils d'experts et une offre de services.

4.1.1.Des conseils d'experts

Crypto.Québec cherche à conseiller sa communauté avec des exemples concrets qui concernent les usages des technologies de l'information et de la communication en lien avec la vie privée. Les conseils peuvent être de nature explicite, par exemple activer une authentification à deux facteurs[37], ou générale, par exemple développer un esprit critique (B6, B1). Les conseils de nature spécifique visent à modifier les manières de faire des usagers dans la vie de tous les jours : gérer ses mots de passe, effectuer régulièrement des mises à jour et sauvegardes de ses appareils, télécharger des applications avec précaution et garder son anonymat. Par exemple, l'organisme invite à prendre le temps d'analyser la liste des applications disponibles sur le marché avant de faire son choix : « Faites vraiment attention [aux] applications gratuites de *VPN*[38] que vous trouvez sur [l'] App Store. [...] On évite ça » (B12). Selon eux, ces

[37] Une fonctionnalité qui permet de protéger un compte avec deux modes d'authentification.
[38] *VPN* pour *Virtual Private Network* ou RPV pour réseau privé virtuel en français. Il s'agit d'un réseau « de communication privée qui peut se servir de l'infrastructure d'un réseau public pour

applications gratuites visent à recueillir des données personnelles sans que les usagers en soient nécessairement conscients : « Quand c'est gratuit, vous êtes le produit » (C8). De plus, Crypto.Québec fournit des conseils pour conserver son anonymat en ligne : désactiver les paramètres Bluetooth et Wi-Fi de son appareil lorsque ces fonctionnalités ne sont pas nécessaires, minimiser les traces en utilisant un navigateur distinct pour Facebook et pour les autres sites Web et utiliser le logiciel Tor pour naviguer sur le Web (B3, B27, F40).

> Si les gens ont un désir de ne pas être espionnés de manière passive[39], je leur recommanderais d'aller sur Tor malgré la mauvaise publicité [...] dans les médias. Ça reste l'un des meilleurs endroits pour préserver son anonymat dans une ère où les entreprises utilisent nos données personnelles non chiffrées pour nous [compartimenter], faire de la publicité ciblée et [nous] vendre quelque chose. (B27)

De plus, les conseils de l'organisme Crypto.Québec vont au-delà de l'utilisation technique d'un appareil. Par exemple, il invite sa communauté à brouiller les traces de sa présence en ligne par la communication de fausses informations : « soyez laconiques » pour les messages d'absence au bureau, utiliser un « flou artistique » pour la géolocalisation dans Instagram[40] et Facebook, mentir « quand ils demandent les courriels » pour l'utilisation du Wi-Fi dans les aéroports (B8, B28, B3).

Les conseils peuvent également être de nature générale et amener les usagers à « développer [...] des bonnes habitudes, [mais] aussi de développer un esprit critique » (B1). Cela se fait notamment par la prise de conscience des enjeux soulevés par l'actualité, mais aussi par le fait de prendre le temps de réfléchir, d'analyser et

---

transmettre des données qui sont protégées grâce à l'utilisation de techniques de chiffrement ou d'encapsulation » (OQLF, 2013).

[39] Crypto.Québec mentionne souvent l'expression « surveillance passive », c'est-à-dire, une « banalisation de la surveillance » (Ouellet et coll., 2015 : 610), où les usagers n'ont rien à cacher et se contentent « de subir les évènements » plutôt que de réagir (CNRTL, s. d.).

[40] Par exemple, un usager pourrait ajouter un lieu sur une photo Instagram qui n'est pas le lieu exact de la prise de sa photo.

d'agir avec précaution dans le monde numérique. Bref, les conseils de l'organisme permettent d'améliorer plusieurs aspects de sa présence en ligne pour faire face au cumul et aux risques liés à la surveillance et à l'identification des données.

4.1.2.Des services pour se rapprocher de la communauté

En plus de ses conseils, Crypto.Québec offre des services au grand public. L'organisme organise à l'occasion des activités thématiques, des évènements en collaboration avec d'autres partenaires et participe à des conférences. En outre, l'activité thématique Crypto.Brunch est une formule qui allie brunch et sécurité informatique, où des formateurs sont invités à répondre à des questions selon les intérêts des participants dans le but « d'améliorer chacun [sa] posture » numérique (A4). Du côté de l'exposition *La chambre de verre*, il s'agit d'un évènement d'une durée de deux semaines organisé en collaboration avec des chercheurs de l'UQAM et d'ailleurs[41] (A14). L'évènement est une adaptation de l'exposition *The Glass Room* de la Fondation Mozilla[42] ayant eu lieu à Londres en 2017 avec des experts « qui s'intéressent aux questions de collecte des données personnelles, de surveillance corporative et d'algorithmes » (A25). Selon l'organisme, cet évènement qui, ironiquement, s'est tenu pendant le scandale de Facebook-Cambridge Analytica, « n'est pas juste une exposition. [...] C'est de voir comment le *Big Data* a pris tellement de place dans nos vies » (A14). Des activités variées sont offertes dans le but de sensibiliser les participants sur leurs traces numériques et de leur fournir des moyens pour se prémunir face à la surveillance des données. Par exemple, Crypto.Québec y tient un Crypto.Party pour apprendre à « sexter avec (plus de) sécurité » et participe à la projection du documentaire *Black Code* sur la « façon dont

[41] Groupe de recherche sur l'information et la surveillance au quotidien (GRISQ) et l'École de sécurité numérique pilotée par Alternatives, la Chaire de recherche du Canada en éducation aux médias et droits humains, la TELUQ et l'ACEI.
[42] Organisme américain sans but lucratif à la défense de l'Internet libre.

les gouvernements à travers le monde manipulent l'Internet pour censurer et surveiller leurs citoyens » (A25).

Durant l'évènement, l'organisme distribue aux participants un guide pour limiter les données produites par leur présence en ligne : « On a une *détox* en 8 jours [...] [où] l'utilisateur peut avoir accès à différents outils pour limiter les traces en ligne. Une journée, par exemple, on va s'attaquer au téléphone cellulaire » (A38) (voir Annexe 4). Ce guide qui est disponible en ligne se décline en plusieurs journées thématiques : « jour 1 : journée découverte – qui êtes-vous selon les autres ? [...] ; jour 5 : connexion – avec qui communique votre téléphone portable ? ; jour 6 : grand ménage – c'est le moment de faire le grand ménage dans les applications » (Data Detox Kit, 2017).

En plus d'offrir des services au grand public, l'organisme propose également des formations aux professionnels intéressés par la sécurité informatique[43]. Dans cet extrait, l'un des membres fait notamment allusion au journaliste Patrick Lagacé de La Presse, qui s'est fait mettre sous écoute par des policiers : « On offre des services puis des formations aux journalistes pour sécuriser les données. [...] Patrick Lagacé et autres journalistes pourraient être intéressés à [ne plus] se faire épier par le SPVM[44] » (A2). Bien que l'OSBL soit basé à Montréal, il est ouvert aux nouvelles opportunités, cherchant à se rendre disponible auprès de sa communauté partout au Québec : « S'[il] y a quelque chose qu'on peut faire [...] vous n'hésitez pas. Vous pouvez nous écrire. [...] On va être là pour vous » (A10).

[43] L'organisme affiche sur leur site une liste des publics intéressés par leurs formations : journalistes, médias, entreprises et cabinets professionnels (Crypto.Québec, 2018).
[44] Acronyme du Service de police de la ville de Montréal.

4.1.3.Les défis

Même si l'organisme use de différents moyens pour aider la population à adopter de meilleures habitudes en ligne, il admet qu'il existe des limites quant à la protection des données. À vrai dire, « la sécurité absolue [n'] existe pas vraiment » (C1). S'il y a des moyens pour se protéger, ils ne doivent pas être considérés comme des « solutions miracles » (*Ibid.*). Malheureusement, même si nous suivons toutes les étapes d'une recette pour naviguer sur le Web en toute confidentialité, il serait toujours possible de nous repérer.

> [*No Place to Hide*][45]. [...] T'as beau être paranoïaque, chiffrer toutes tes communications, pas avoir de compte Facebook, [...] même sans compte Facebook on fait beaucoup de données quand même juste à naviguer sur Internet. [...] On [ne] s'en sort pas. (*Ibid.*)

De plus, chercher à brouiller sa trace en ligne peut conduire à l'effet inverse de l'anonymat. Particulièrement parce qu'une personne qui masque ses usages par le biais d'un logiciel spécialisé peut être repérable dans une masse d'internautes qui n'emploient pas ledit logiciel : « Dans une foule de 100 000 personnes avec des masques, on ne sait pas qui vous êtes. Si vous êtes le seul avec un masque, [on va le savoir] » (C34).

Également, Crypto.Québec note les limites des appareils utilisés pour naviguer en ligne. La plupart du temps, les fabricants les ont conçus de manière à rendre opaques les pièces et les processeurs qui se trouvent à l'intérieur : les « cellulaires, c'est des systèmes fermés » (C1). Nous ne connaissons pas le potentiel de ce qu'ils renferment. En ce sens, l'organisme donne l'exemple des senseurs internes d'un téléphone

[45] L'organisme fait allusion au livre de l'auteur Gleen Greenwald à propos de sa rencontre avec Edward Snowden (2014).

intelligent (magnétomètre, baromètre, etc.) qui permettent de suivre une personne, même lorsque la fonction de géolocalisation est désactivée (C12)[46].

De plus, un autre défi est l'incapacité à prévoir les conséquences de l'utilisation des données par les entreprises. Par exemple, la carte de densité de l'application mobile Strava[47] avec « les activités partout dans le monde de leurs clients [...] entre 2015 et 2017 » souhaitait révéler un portrait mondial de l'activité physique, mais a finalement permis la découverte de bases militaires secrètes américaines (C11). Même chose pour Snapchat[48], un média socionumérique populaire auprès des adolescents, qui avait lancé une fonctionnalité pour voir en temps réel la localisation de son réseau d'abonnés, remettant en question la confidentialité sur sa plateforme : « C'est qu'on est vraiment capable de suivre quelqu'un dans sa journée de très, très, très près là » (C28).

Aussi, la valeur commerciale attribuée à nos données est un défi et l'organisme le sait bien. Par exemple, les médias socionumériques sont conçus de manière à extirper des données en échange d'un service « entre guillemets gratuit [...] [et] font leur argent [...] en revendant les données personnelles des gens. [...] C'est le modèle d'affaires de la [...] *Surveillance Valley* » (C37). Parlant de chiffres, Crypto.Québec mentionne que Facebook fait environ « 3,82 $ par année par utilisateur sachant qu'ils ont plus

[46] L'organisme fait référence à une étude américaine : *PinMe: Tracking a Smartphone User around the World* (Mosenia et coll., 2017).

[47] Strava est un média socionumérique utilisé à travers le monde par les coureurs et cyclistes. Ils peuvent y recueillir des données sur leurs activités sportives, notamment avec une carte de leurs parcours.

[48] Snapchat est une application mobile basée sur le partage de contenus (photo ou vidéo) éphémères, c'est-à-dire des messages qui disparaissent après une durée de vie déterminée par l'usager. Il est également possible de créer des publications de type « Story » qui s'efface après une durée de 24 heures.

d'un milliard d'utilisateurs » (*Ibid.*)[49], et que la valeur d'achat d'une identité numérique est évaluée à environ 1 170 $ US sur le *dark web*[50] (C14).

Enfin, il est à noter que les conseils promus par l'organisme ne sont pas sans risques. Nous relevons deux exemples qui portent sur l'utilisation de Tor[51], un logiciel qui tend à permettre la navigation de façon « anonyme »[52] – l'anonymat sur Tor est remis en question après la révélation de liens étroits avec la sécurité nationale des États-Unis (Levine, 2018) – sur les sites non répertoriés par les moteurs de recherche traditionnels (ex. : Google). Dans le premier cas, l'un des membres avoue être craintif suite à l'arrestation d'un opérateur de relai de sortie Tor[53] : « Quand je lis ce genre de nouvelle là qui *pop-up* [...] j'ai toujours un frisson parce que je suis moi-même un opérateur de relai de sortie Tor. [...] La police va venir frapper à ma porte en premier » (C2). Dans le second cas, la crainte est dirigée vers la communauté. Il est mentionné que la mise en place d'un nœud de sortie Tor peut s'avérer complexe et dangereuse. Par conséquent, les recommandations de Crypto.Québec ne doivent jamais être prises à la légère : « Ne prenez pas nos réponses parfois un peu courtes par rapport à [Tor]. [...] Ça peut mettre la vie de gens en danger [...] si [ce n'] est pas fait correctement » (*Ibid.*).

---

[49] Une autre étude parle même de 20,21 $ US par usager par année avec 1 401 000 000 usagers actifs sur Facebook en 2017 (Statista, 2018a ; Statista, 2018b).

[50] Une partie du Web qui ne fait pas partie des recherches indexées dans les navigateurs traditionnels (OQLF, 2017).

[51] Le logiciel Tor fonctionne à partir d' « une série de relais créés par des utilisateurs du réseau un peu partout dans le monde avant de finalement aboutir au serveur voulu, le tout en se servant de communications chiffrées » (Ici Radio-Canada, 2018). Il est donc difficile de retracer celui qui a initié la première connexion.

[52] Comme le dit Crypto.Québec, « la sécurité absolue [n'] existe pas vraiment » (C1). Ainsi, même l'anonymat sur le réseau Tor peut être démasqué. Nous relevons l'exemple du fondateur de Silk Road, un marché noir sur Tor, qui a été retrouvé et arrêté par le FBI (Bearman, 2015).

[53] Par souci de sécurité, le trafic de chaque usager est acheminé au réseau Tor par l'entremise de « trois serveurs aléatoires (aussi appelés relais). [...] Le dernier relais du circuit (le « relais de sortie ») envoie ensuite le trafic vers l'Internet public » (Tor, 2018).

4.2. Influencer les décisions de demain

Crypto.Québec prend également des mesures pour élargir la portée de sa mission. Sachant que les usagers, de par leurs données, sont présentement exploités par les compagnies technologiques, l'organisme essaie de mettre en lumière ce contexte défavorable. Il n'existe pas nécessairement de modèle ni d'organisation similaire au Québec. Or, observant la demande pour leurs services, par les questions du public ou leurs interventions dans les médias, il cherche à se donner les moyens nécessaires pour structurer le lieu de leur terrain de jeu et poursuivre leur trajectoire.

Premièrement, au niveau de l'organisation interne, les membres se sont dotés d'un conseil d'administration et d'un conseil exécutif pour mener à bien les orientations stratégiques et différents projets de l'organisation : « Il était temps d'optimiser les ressources de l'organisme afin de multiplier les projets prometteurs et de défendre plus efficacement nos libertés individuelles et collectives » (D17). Cette structure répond aux exigences des OSBL et permet d'intégrer de nouveaux membres au sein de l'équipe afin de perpétuer la mission de l'organisme. Depuis sa création en 2015, l'organisme « est [passé] de trois bénévoles à une vingtaine » (*Ibid.*).

Deuxièmement, l'organisme travaille sur un livre collectif pour « introduire les principes de base de la sécurité numérique à un large public » (D24). Le but de ce livre n'est pas d'aller « dans les détails techniques », mais plutôt de sensibiliser le public à la sécurité informatique pour mieux « se prémunir des risques relatifs à un environnement numérique vulnérable » (D26, D24). Il faut dire que les conseils qui proviennent de Crypto.Québec ne sont pas nécessairement enseignés à l'école ni au travail. Inversement, il serait étonnant que les fabricants et les compagnies technologiques informent leurs usagers sur les moyens employés par l'organisme Crypto.Québec pour protéger sa vie privée en ligne, et ce, tout aussi longtemps que

leur modèle d'affaires sera basé sur la récolte des données. Avec la publication d'un livre, Crypto.Québec cherche à fournir un premier guide aux usagers pour circuler plus librement (du moins en partie) sur le Web.

Troisièmement, comme nous l'avons vu, l'organisme travaille étroitement avec des médias, des partenaires, des chercheurs, mais s'associe aussi à des organisations qui lui ressemblent à l'international. Il « a signé conjointement avec quelque 83 groupes de la société civile une lettre pour se prononcer face aux discussions menées par les gouvernements des *Five Eyes*[54] » (D22). Cette revendication fait suite aux discussions de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis qui cherchaient à contrevenir à des attaques potentielles de terroristes en ayant recours plus facilement aux données des usagers en ligne. Aux côtés d'organisations civiles comme *Electronic Frontier Foundation* et *The Tor Project*, Crypto.Québec a cosigné la lettre dans le but de faire pression auprès des gouvernements pour faire respecter le chiffrement des communications : « C'est Jacob Appelbaum[55] qui avait dit à un moment donné qu'on ne va pas interdire les routes parce qu'il y a des terroristes qui se promènent sur les routes » (D7).

4.2.1.Réfléchir à de nouveaux modèles d'affaires

Lors d'une entrevue à l'émission *Tout le monde en parle* sur Ici Radio-Canada (2018), l'un des membres fondateurs de Crypto.Québec, Luc Lefebvre, discute avec Patrick Lagacé, journaliste à La Presse, des pratiques en matière de protection des données. Au Québec, nous n'observons pas de discussion à proprement dit sur les données et la France semble être en avance à ce sujet. Le journaliste fait allusion au

[54] Aussi connu sous l'expression « groupe des cinq ». Il s'agit d'une « communauté de la défense composée de l'Australie, du Canada, des États-Unis, de la Nouvelle-Zélande et du Royaume-Uni » (Gouvernement du Canada, 2018).
[55] Chercheur américain considéré comme l'un des principaux développeurs du projet Tor.

Règlement général sur la protection des données (RGPD)[56] en Europe qui vise à « donner plus de pouvoir aux usagers sur leurs données [et] plus de contrôle [...] dans ce qui est présentement une sorte de *Far West* » (D43). Il y a lieu de reconsidérer les modèles d'affaires en place. Pour ce faire, il faudrait appliquer de nouvelles règles au Québec et, par le fait même, faire pression sur les entreprises actuelles. Si nous accordons une certaine valeur commerciale aux données, le journaliste cite sans le nommer un philosophe français qui avait émis l'idée que les usagers soient payés pour les données qu'ils génèrent (*Ibid.*)[57]. Luc Lefebvre de Crypto.Québec soulève également l'exemple d'un autre modèle d'affaires :

> Tu [ne] veux pas que Google utilise tes données ? [...] Bien, paye par mois. Il y a probablement plein de monde qui dirait : [...] j'ai envie de payer 10 $ par mois [...], mais [...] en échange il [ne] prenne pas mes données puis [il ne] les revende [pas]. [...] Y'aurait plein de possibilités [...] [ou de] modèles d'affaires qu'on pourrait parler [...] si on avait la discussion. (*Ibid.*)

Pour que ces nouveaux modèles économiques soient mis en branle, il faut d'abord que les Québécois s'intéressent à la question pour ensuite faire pression sur le gouvernement et sur les entreprises.

4.2.2.Les défis

4.2.2.1. Peu de débats au Québec selon l'organisme

D'abord, la société québécoise ne se sent pas encore concernée par les questions entourant la gestion des données numériques. Depuis quelques années, l'insertion des

[56] Le règlement est entré en vigueur le 25 mai 2018.

[57] Nous pensons qu'il fait référence au rapport *Mes data sont à moi* du groupe de réflexion GénérationLibre, dirigé par le philosophe français Gaspar Koenig : « L'utilisateur devrait pouvoir refuser ce modèle économique, quitte à payer pour l'utilisation des outils jusqu'alors gratuits, mais en revanche être payé pour la fourniture de ses données personnelles » (Koenig et coll., 2018).

médias socionumériques s'est faite graduellement dans nos vies sans remettre en question leurs intentions. Comme le mentionne Crypto.Québec : « On n'est plus des victimes de ce qu'on pourrait appeler de [la] surveillance passive » (E43). Nous pouvons comprendre la surveillance passive comme le fait d'être l'objet d'une observation attentive de nos traces numériques par les entreprises et les gouvernements, et ce, sans réagir. De fait, les Québécois sont en général naïfs quant à la surveillance ou l'espionnage exercés sur leurs données : « On n'a jamais vraiment eu la discussion sur qui qui surveille, ce qui nous surveille et qu'est-ce qui arrive avec tout ce que j'utilise » (*Ibid.*). Avec l'Internet des objets et des appareils connectés qui s'insèrent de plus en plus dans nos vies, l'organisme met en garde contre l'écoute passive. Par exemple, un haut-parleur intelligent (Google Home, HomePod d'Apple, Echo d'Amazon, Sonos, etc.) qui permet de contrôler des applications et des appareils connectés par la voix : « Un dispositif qui est dans ta maison et qui t'écoute tout le temps [...] puis toutes ces données peuvent être stockées sur des serveurs Google [...] aux États-Unis [où] les lois c'est le *Far West* » (*Ibid.*).

De fait, personne n'oblige quiconque à utiliser les médias socionumériques. Comme le fait remarquer Patrick Lagacé, ces moyens sont tellement ancrés dans les habitudes des Québécois qu'ils deviennent « quasiment un service public » (*Ibid.*). C'est pourquoi le journaliste se dit préoccupé de l'état de la situation :

> Il faut que l'État mette des barrières puisque présentement, c'est une sorte de *Far West.* [...] Tu vois [...] une sorte de capture cognitive entre l'État canadien et les géants du Web. C'est comme s'[ils] ne peuvent pas avoir tort, ne peuvent rien faire de mal et ça, comme citoyen, moi, ça m'inquiète beaucoup. (*Ibid.*)

Au Québec, il y a le Commissariat à la protection de la vie privée du Canada et la Commission d'accès à l'information du Québec qui régissent la protection des données détenues par des organismes et des entreprises privées. Néanmoins, selon les

dires de Crypto.Québec, ces organisations ne semblent pas avoir le pouvoir pour faire face aux géants du Web : « par exemple quelqu'un [...] qui se fait hameçonner. [...] [Ils] n'ont pas les ressources financières ou techniques pour [...] jouer un peu le rôle de shérif dans ce *Far West* » (*Ibid.*). Pendant ce temps, les GAFAM profitent de cette surveillance passive.

4.2.2.2. Des ressources limitées pour Crypto.Québec

Le contexte dans lequel prend part Crypto.Québec est exigeant. L'actualité ne tarit pas dans le monde numérique qui présente constamment de nouvelles technologies. Ce faisant, les individus cherchent à s'informer davantage sur le sujet : « Les crises et les attaques se multiplient, les citoyens, médias, entrepreneurs et élus politiques ont plus que jamais le besoin d'avoir accès à des ressources et à des explications techniques sur ces phénomènes complexes » (E24). Par conséquent, les membres de l'organisme, qui jonglent entre leur vie personnelle, leur occupation professionnelle et leur rôle de bénévole auprès de Crypto.Québec, doivent mettre les bouchées doubles pour continuer à faire rayonner l'organisme.

> Parmi tous les collaborateurs d'un organisme qui [sont] bénévoles, on se donne et on écrit un livre, on fait des conférences, le ciel est en feu dans les médias depuis des semaines, on est un [...] peu fatigué. [Il] va peut-être falloir qu'on change notre rythme. (E15)

Les membres dépendent principalement du soutien des donateurs pour financer leurs activités, dont la production de contenu et de formations. Par exemple, l'organisme rappelle que les bons commentaires qu'ils reçoivent pour leur balado sont vus comme une forme de paiement : « C'est apprécié, il ne faut pas oublier qu'on est un OSBL, on [ne] fait pas ça à temps perdu. [...] À défaut d'avoir du financement, c'est une source de revenus intéressante et on vous [en] remercie » (E6).

4.3. De l'individu à la société

Les moyens utilisés par l'organisme pour changer les habitudes des individus et influencer les décisions au niveau de la société sont parfois interreliés. Crypto.Québec se rend compte qu'il ne faut pas seulement conscientiser la population, mais également influencer les décisions prises par les entreprises et gouvernements pour arriver à ses fins. Son idéal serait de ne plus avoir à intervenir. Toutefois, comme la route est longue, il y a un certain pessimisme qui se dégage du discours de Crypto.Québec :

> L'actualité ne tarit pas, moi j'aimerais ça qu'on ne serve plus à rien, qu'il y ait de l'information factuelle sur le *hacking* dans les médias, que la surveillance de masse se fasse dépecer à petits morceaux, qu'on en arrive à quelque chose qui est socialement acceptable qui respecte la vie privée, puis que les gens apprennent à avoir des bonnes pratiques pour améliorer leur posture, mais en attendant vous êtes *pluggés* avec nous. (F8)

4.3.1. De la prise de conscience individuelle à des changements collectifs

L'organisme qui mise sur la collectivité et les actions menées par les individus se doit également de faire pression sur les entreprises. Celles-ci profitent présentement d'un flou en termes de règlementation, de la méconnaissance de leurs usagers quant à la récolte des données et du respect de leur vie privée : « l'absence de protection des données égale modèle d'affaires de la Silicon Valley présentement » (E11).

L'organisme invite à mettre en application la résistance pour pouvoir développer une prise de conscience : « Grognez avec nous ! Soyez des chiens de garde ! » (F12). Ces actions de résistance peuvent s'avérer anodines, mais elles peuvent mener à une

réflexion plus profonde sur les droits d'une personne. Par exemple, le refus de montrer son sac à l'entrée de sécurité d'un festival si nous jugeons que nous n'avons rien à cacher ou nous ne souhaitons pas montrer nos effets personnels (F7). Parallèlement, cette prise de conscience pourrait être reproduite en ligne, notamment pour réfléchir sur l'utilisation des données et sur les façons de limiter les traces de sa présence en ligne et de résister à la surveillance. Cette représentation de la réalité peut faire peur, mais elle peut, selon l'organisme, nous mener à des changements bénéfiques sur Internet : « La paranoïa a sa place dans l'optique que c'est important d'être critique par rapport à ça. [...] L'objectif c'est [...] de penser critiquement [sic][58] à ce qu'on peut, puis essayer d'être conscient, puis d'adopter des habitudes qui peuvent minimiser tout ça » (F35).

Si chaque individu se pose des questions et devient de plus en plus conscient, nous pourrions assister à un éveil collectif, un rassemblement d'individus responsables et soucieux de leurs données, qui par leur nombre pourrait résister aux manières de faire des compagnies technologiques et les amener à repenser leurs modèles d'affaires en fonction des usagers et non pour leur valeur accordée : « Si c'est financièrement non viable pour les entreprises de continuer à vendre des dispositifs qui espionnent de même, ils vont arrêter de le faire » (F12).

Avant d'y arriver, Crypto.Québec invite la communauté à changer ses habitudes graduellement. Nous pouvons nous intéresser au sujet, changer peu à peu nos habitudes et prendre part à un mouvement collectif : « C'est des étapes, c'est une recette [...] [il] y a des Crypto.Party, des formations, mais [il] y a aussi la pratique » (F3). Ces gestes doivent également aller au-delà du simple fait de fermer son compte Facebook pour avoir une meilleure vie privée. Il faut trouver d'autres moyens plus tangibles pour faire face à ces compagnies. Il faut s'y intéresser, les

[58] Expression exacte est « de façon critique ».

comprendre et ne pas hésiter à les remettre en question : « [Il] faut vraiment se retourner vers ces entreprises et leur demander [si] on trouve ça correct comme société de permettre à ces mégas entreprises [...] d'accumuler autant d'informations sur nous » (F37).

L'usager doit non seulement comprendre les données et tenter de réduire les traces qu'il génère sur Internet, mais il doit également s'unir avec d'autres personnes pour arriver à des changements significatifs et faire évoluer la société : « [Il] y a beaucoup qu'on peut faire, donc c'est de la pression sociale, c'est changer sa culture par rapport au numérique » (F40). Certains pourraient se demander la pertinence de s'opposer à ceux qui récoltent des données, comme quoi le combat est déjà une peine perdue, mais pour Crypto.Québec, il ne faut pas désespérer et chercher à reprendre graduellement le contrôle de sa vie numérique :

> Ça vaut vraiment la peine [d'avoir des courriels différents ou de faux noms] parce que c'est des façons de compartimenter. Oui, ça devient des identités qui sont séparées, mais au moins, on garde le contrôle [...] [puis] ça, c'est une habileté qui se perd. Au temps de la Guerre froide [...] les gens avaient ce réflexe-là, de ne pas dire n'importe quoi à n'importe qui [...] [et] quelle est la conséquence [...] si je révèle que mon ami est avec moi dans un party. (F42)

4.3.2.Des *hackers* à l'enseignement universitaire

Crypto.Québec se réjouit que les universités s'intéressent de plus en plus aux enjeux de la sécurité informatique. Pour brouiller les traces de sa présence en ligne, nous avons maintenant des chercheurs qui s'intéressent à des moyens pour le mettre en pratique. L'organisme fait notamment allusion au colloque *International Workshop*

on Obfuscation[59] s'étant déroulé en avril 2017 à l'Université de New York : « On est rendu au point où [...] des conférences en informatique sont [...] sur comment faire de l'*obfuscation*. [...] C'est intéressant de voir qu'il y a de la recherche qui se fait là-dessus. La résistance s'organise » (F3). Il est également mention du livre *Obfuscation: A User's Guide for Privacy and Protest* (2015), écrit par deux chercheuses de ladite conférence, qui offre un guide pratique à tous ceux et celles qui désirent obscurcir leur présence en ligne.

[59] L'obscurcissement est défini comme « l'ajout délibéré de données ambiguës, confuses ou trompeuses pour entraver la surveillance et la collecte de données [traduction libre] » (Brunton et Nissenbaum 2016 : 1).

CHAPITRE 5

INTERPRÉTATION DES RÉSULTATS

Suivant la présentation des données, nous interprèterons nos résultats de recherche en lien avec notre problématique et notre cadre théorique. Nous chercherons à dégager les pistes de réflexion découlant de nos résultats, de façon à mieux répondre à nos questions de recherche.

5.1. Le circuit marchand des mégadonnées au cœur des discussions

Crypto.Québec met en lumière le contexte actuel du circuit marchand des mégadonnées abordées dans notre problématique. Nous retrouvons dans leur discours certaines des caractéristiques principales des mégadonnées, comme l'expression *capta*, au sens où les données « en volume et en variété » sont prises et exploitées par les entités tierces, notamment pour créer une « valeur » commerciale.

En matière de « valeur », l'organisme cite un dicton que l'on entend depuis quelques années dans les médias (La Quadrature du Net, 2016 ; Adesias, 2013) : « quand c'est gratuit, *vous* êtes le produit ». En effet, les plateformes en ligne offrent souvent des services dits « gratuits » en échange de données personnelles. Les usagers qui entrent dans ces circuits marchands participent à la production, à la captation et au traitement

de leurs données par des usages prédéterminés par les entreprises du GAFAM. Ainsi, les entreprises privées cherchent à combler leurs intérêts économiques en dépit des intérêts des individus.

D'ailleurs, peu de gouvernements cherchent à s'opposer à la manière dont les entreprises privées régulent leurs plateformes (à l'exception du *Règlement général sur la protection des données* en France), ce qui laisse libre cours à leur quête perpétuelle de données. Comme il y a peu d'instances qui s'en inquiètent, il y a peu de voix qui s'élèvent pour sensibiliser la population. Cette dernière tient alors les plateformes en ligne (médias socionumériques, applications, etc.) pour acquises, les utilisant avec insouciance. Un individu voit sa famille, ses amis, ses collègues qui les utilisent au quotidien, alors pourquoi serait-il porté lui-même à les remettre en question ? « Tout le monde le fait ». Il semble normal, par exemple, que Facebook offre un service gratuit en échange de données pour pouvoir ensuite les revendre en publicité. Il semble normal que les usagers utilisent cette même plateforme sans se questionner, ni même lire les conditions d'utilisation, pressés par les bénéfices qu'ils peuvent en retirer.

Or, pour Crypto.Québec, cette situation ne devrait pas être prise à la légère. L'organisme est préoccupé par la « surveillance passive » et l'indifférence de la population. Les usagers ne sont pas suffisamment conscients de l'étendue des traces qu'ils produisent en ligne. Ils se laissent surveiller par des entités tierces sans même y réfléchir. Les entreprises du GAFAM cherchent à décourager ceux qui se questionnent par la mise en place d'infrastructures lourdes, complexes et inaccessibles. Par conséquent, les usagers adoptent la « non-tactique » (*op. cit.*, Martínez, 2017 : 7). Indifférents, ils succombent aux usages mis en place par les entreprises. Selon Crypto.Québec, il faut éveiller la population sur les enjeux de surveillance et de vie privée. La communauté doit être mieux informée à propos de l'usage de ses données, en discuter, chercher à comprendre et à reprendre le contrôle

de sa vie privée en ligne pour, finalement, faire valoir ses libertés individuelles et collectives.

En ce qui a trait aux caractéristiques « volume » et « variété » des mégadonnées, Crypto.Québec constate que les plateformes en ligne sont ancrées de plus en plus dans les habitudes de vie. Pour reprendre les mots du journaliste Patrick Lagacé, nous avons des médias socionumériques comme Facebook qui sont devenus pratiquement des « services publics ». Si bien qu'il est presque impossible aujourd'hui de ne pas produire de données. Sortir de la maison pour aller prendre le métro peut permettre à notre téléphone intelligent de capter nos déplacements. Même lorsque nous désactivons Bluetooth ou la géolocalisation, Crypto.Québec mentionne que d'autres mécanismes internes au téléphone intelligent permettent de recueillir des données.

De plus, les gouvernements savent que les plateformes en ligne détiennent une mine d'or de données sur la population. Si nous avions Edward Snowden qui, en 2013, révélait les accès de l'Agence nationale de la sécurité américaine (NSA) aux données des géants de la Silicon Valley (Google, Facebook, etc.), nous avons encore aujourd'hui des gouvernements qui cherchent par de nouveaux moyens[60] à se procurer les données des usagers. C'est pourquoi des organismes comme Crypto.Québec continuent à s'opposer aux gouvernements qui cherchent à profiter des informations sur les utilisateurs d'Internet.

[60] C'est le cas des *Five Eyes* qui cherchent à contrevenir à des attaques potentielles de terroristes en ayant recours plus facilement aux données des usagers en ligne (D22).

5.2. Les GAFAM et le mode de reproduction décisionnel-opérationnel

Après avoir abordé le contexte du circuit marchand des mégadonnées, nous retrouvons également des caractéristiques du mode de reproduction décisionnel-opérationnel de Freitag dans le discours de Crypto.Québec. Premièrement, les membres de l'organisme font état de la logique opérationnelle, capitaliste et marchande entourant l'usage des plateformes en ligne. Les individus accèdent à des sites Web ou des applications mobiles « entre guillemets gratuits » (C37), mais, en contrepartie, ils réduisent l'ensemble de leurs faits et gestes en de simples unités de mesure informatiques. Ces traces peuvent servir à créer des profils quantifiables et monnayables (*op. cit.*, Filion, 2006 : 264), comme par exemple avec le profilage et le ciblage publicitaire qui profitent aux entreprises du GAFAM et leurs partenaires.

Deuxièmement, les individus jouissent des bienfaits que leur procurent les plateformes en ligne, sans nécessairement les remettre en question, adoptant « un rapport immédiat au monde sans réflexivité ni sens » (*op. cit.*, Baillargeon, 2009). Par exemple, les médias socionumériques proposent des fonctionnalités qui plaisent, divertissent et paraissent bien utiles. Ces plateformes en ligne – souvent gratuites – ne donnent pas d'autre choix à l'usager que de fournir des données comme monnaie d'échange pour y accéder : « Quand on télécharge une application, on [ne] lit pas [les conditions d'utilisation], c'est très compliqué, le rapport de pouvoir [n'] est pas le même, c'est un choix d'utiliser l'application ou de ne pas l'utiliser » (H35). En général, ces conditions d'utilisation sont écrites de façon à permettre aux entreprises privées de récolter des données sur leurs usagers. Rappelons que l'usager qui accède à Internet est entouré d'une abondance de conditions d'utilisation qui d'une part, sont écrites dans un langage juridique non accessible, et d'autre part, sont trop nombreuses pour être lues avec une attention soutenue. Cela fait en sorte que les conditions

d'utilisation peuvent ne pas être bien comprises par l'usager moyen. Crypto.Québec s'inquiète du fait que la population est généralement naïve et indifférente à l'égard de la surveillance passive qui est exercée sur leurs données (E43). La population est-elle si insouciante ou bien seulement désavantagée, ou même dépassée, par la manière dont ont été conçues les plateformes en ligne et leurs conditions d'utilisation ?

Ainsi, la meilleure manière de ne pas dévoiler ces données est de se déconnecter. Par contre, pour l'organisme, les plateformes en ligne telles les médias socionumériques deviennent parfois indispensables par leur utilité et il peut être difficile de s'en séparer :

> Si on *delete* notre compte Facebook, puis qu'on va quelque part d'autre, on minimise les données qu'on fait sur nous. [...] Mais ce n'est pas tout le monde qui a ce luxe-là. Facebook, pour plusieurs, ça reste la seule manière de rester en contact avec des personnes. (H38)

Troisièmement, un autre élément caractéristique du mode de reproduction décisionnel-opérationnel est le fait que les GAFAM s'inscrivent dans le contexte postmoderne, loin de l'idéologie des grands principes (la raison, la liberté, les droits de l'homme, etc.) (*op. cit.*, Filion, 2006 : 175). Ce qui intéresse ces entreprises privées, c'est l'esprit même du capitaliste et son expansion sans fin : accumuler toujours plus de capitaux par le cumul d'abonnés et par le nombre de données qu'ils peuvent en soutirer. Pour Crypto.Québec, ce modèle d'affaires est « une sorte de *Far West* » (D43) qui signifie au sens familier, l' « endroit où règne la loi du plus fort » (Larousse, s. d.). Dans le fond, les usagers circulent à travers un système technique beaucoup plus vaste qu'eux, qui ne vise pas forcément à satisfaire leurs intérêts propres, mais plutôt à faire profiter toujours davantage les entreprises privées.

En résumé, les entreprises du GAFAM contrôlent un système technique où les décisions qui y sont prises et les opérations qui en découlent sont motivées par la

recherche de profit. Nous pouvons penser que ce circuit marchand se reproduit dans le temps sans pouvoir être significativement modifié ou altéré par les usagers. Par contre, cela n'arrête pas l'organisme Crypto.Québec qui s'affaire à vulgariser les enjeux numériques, dénoncer les sujets de pouvoir et fournir des conseils et des services à tous ceux qui souhaitent y faire face.

5.3. Les rapports de pouvoir et les points de fuite : des conseils et des services comme tactiques de détournement

5.3.1. Les protagonistes

Dans le discours de Crypto.Québec, nous retrouvons des protagonistes impliqués de près ou de loin dans leurs activités ou dans l'actualité médiatique. Cela offre notamment un aperçu des rapports de pouvoir qui se créent parmi les protagonistes.

Nous avons d'abord le citoyen numérique : celui qui navigue sur Internet, qui utilise les plateformes en ligne et qui a une valeur commerciale en matière de données. Il fait partie des victimes de la « surveillance passive » et des failles informatiques, par exemple, les « 1,9 million d'enregistrements des clients » de la compagnie de télécommunication Bell qui ont été dérobés en 2017 lors d'un piratage informatique (E43, G11).

Nous avons ensuite les entités qui entourent le citoyen numérique. Premièrement, nous avons les grandes compagnies technologiques, notamment les GAFAM (Google, Amazon, Facebook, Apple et Microsoft). La perception que Crypto.Québec a face aux entreprises technologiques n'est pas nécessairement favorable. Bien qu'elles proposent des plateformes qui cherchent à rendre la vie meilleure, de la

communication au divertissement, l'organisme se préoccupe de la collecte des données :

> Ce qui est beaucoup plus épeurant, c'est tout ce qui est la captation passive que tout le monde subit à tous les jours constamment, au niveau de l'envoi de nos recherches Google, tout ce qui est *browser history*, les *web beacon*[61] qu'on transfère d'un site Web à un autre. (G1)

Ces entreprises ne sont pas basées sur la liberté individuelle, mais plutôt sur des intentions commerciales, avec la valeur monétaire que peut leur fournir la surveillance des usagers de leurs bases de données : « de la même façon qu'on dit aux gens : [...] [ne] dites pas sur Facebook que vous allez en vacances [...], [il y] a une base de données qui sait quand vous [n'] êtes pas chez vous » (G3). Deuxièmement, nous avons aussi d'autres entreprises qui parfois, sans prendre suffisamment de précautions, récoltent des données sur leurs usagers. Nous relevons notamment Disney et sa poursuite « pour avoir contrevenu aux lois pour la vie privée des enfants », ainsi que Bell et Strava nommés précédemment (G8, 11). Troisièmement, nous pouvons retrouver les entités gouvernementales (municipalité, corps policiers, etc.) qui possèdent des données sur les citoyens numériques (G2, H1).

Les *hackers* sont aussi mentionnés dans le discours de l'organisme, notamment les personnalités bien connues dans le monde des cyberactivistes comme Edward Snowden, lanceur d'alerte de la NSA, ou Jacob Appelbaum, chercheur et développeur lié à Tor. Il est aussi question du cheminement des membres de l'organisme. À la question « pour faire carrière en cybersécurité, quels sont les meilleurs moyens de s'éduquer sur le domaine : formation, certification, programme, etc. ? » (G5), certains des membres de Crypto.Québec parlent de leur parcours en lien avec la cybersécurité. L'un d'eux fait une description technique des travailleurs dans ce domaine : les

[61] Le pixel espion est une petite image invisible d'un pixel qui est activée lors du téléchargement d'une page. Il est utilisé pour suivre et collecter des informations sur l'usager (OQLF, 2002).

purple team, les *blue team* et les *red team*. Cette nomenclature en trois groupes est notamment utilisée par les militaires : les *red team* cherchent à attaquer un territoire, les *blue team* tentent de défendre leur territoire et les *white team* favorisent les échanges entre les deux groupes (Schneider, 2003 : 9). Le *white team* est ici appelé *purple team* par Crypto.Québec, et cette équipe agit à titre de médiatrice avec leurs deux autres équipes.

> Je suis plus un gars de *blue team.* [...] C'est [la] défense d'infrastructure. [...] La sécurité représente entre 40 et 50 % de ma *job*. [...] J'ai des certifications, [...] [mais] l'autodidactisme est une qualité nécessaire à avoir dans cette industrie. L'informatique en général c'est pas assez de faire du 9 à 5, [il] faut que tu en manges. [...] Je m'en vais vers le *purple team*, [...] le mix entre *blue team* puis le *red team*. Le *red team* c'est ceux qui attaquent puis les bleus c'est ceux qui défendent. (G5)

Il n'est pas nécessaire de connaître les codes informatiques en détail pour devenir un *hacker*. Il est possible d'être un *hacker* autrement. Par exemple, l'un des membres se dit « *hacker* d'humains » dans la mesure où il gère et supervise des projets informatiques (ex. : détection de faille sur une application) et travaille étroitement avec des individus qui ont les capacités techniques (G5). Bien que leur perception des *hackers* soit relativement bonne, les membres de Crypto.Québec sont conscients que ceux qui pratiquent le métier ou s'intéressent au sujet peuvent être jugés défavorablement dans la société : « On entend [souvent que] le chiffrement [des données] c'est pour les gens qui [n'] aiment pas la police, [...] des méchants. [...] Un courant qui tend à démoraliser [...] des organismes comme nous » (I7).

D'autres protagonistes comme les médias occupent une place prépondérante dans les discours de Crypto.Québec. Ils sont en quelque sorte leurs alliés, où, dans un rapport gagnant-gagnant, le discours de l'organisme augmente sa portée grâce aux médias et les médias augmentent leur crédibilité avec l'apport d'un organisme qui peut vulgariser l'information du moment. Ainsi, comme l'organisme est souvent invité à

commenter l'actualité, il entretient de bons rapports et des liens étroits avec les médias. Sinon, l'organisme n'indique pas clairement qui sont leurs autres alliés, mais nous pouvons penser à quelques sympathisants. En tant qu'utilisateur du logiciel Tor et participant à une conférence avec des développeurs de *The Tor Project*, l'organisme agit à titre d'ambassadeur dans la mesure où il invite d'autres utilisateurs à contribuer à la plateforme : « J'en profite pour inviter les gens, si vous avez les capacités techniques, rouler des nœuds de sortie, surtout Tor, si possible, le réseau a besoin de vous » (I2). Leurs alliés seraient également les organisations qui lui ressemblent à l'international (pétition signée avec plus de 83 organisations) et le milieu universitaire avec qui il collabore.

Pour ce qui est de leurs adversaires, nous retrouvons ceux qui peuvent compromettre la sécurité en ligne et la vie privée des usagers : les « rançongiciels » telles WannaCry et les failles informatiques comme Spectre et Meltdown (J8, 10, 19). Sinon, nous pouvons retrouver les entreprises et gouvernements qui ne se soucient pas nécessairement des usagers, mais plutôt de leurs données. Néanmoins, c'est en raison des failles informatiques, des arnaques ou de la surveillance des données que l'organisme a raison d'être et est invité à commenter l'actualité.

Bref, nous retrouvons dans le discours de Crypto.Québec différents protagonistes : citoyens numériques, entreprises privées du GAFAM, entités gouvernementales, *hackers*, médias, organisations de sensibilisation, etc.

5.3.2.Les rapports de pouvoir et les points de fuite

En nous inspirant de la notion de gouvernementalité de Foucault, nous pouvons observer l'existence de rapports de pouvoir entre les protagonistes mentionnés par

Crypto.Québec. C'est notamment en prenant connaissance de ces rapports de pouvoir que nous pouvons chercher les points de fuite possibles pour les modifier.

Premièrement, nous avons les entreprises du GAFAM qui entretiennent un rapport dominant face aux citoyens numériques. Ils cherchent à déterminer la conduite de leurs usagers par l'entremise de stratégies. Par exemple, ils utilisent des instruments d'observation (conditions d'utilisation, algorithmes, etc.) qui leur permettent de voir tout ce qui peut être gouverné à travers les traces numériques laissées par leurs usagers. De fait, les entreprises privées ont conçu un circuit marchand pour que les usagers puissent y circuler à découvert avec leurs données. Il n'y a souvent pas place à un débat social à l'intérieur de ces plateformes, car les conditions d'utilisation qui y sont proposées doivent être acceptées pour profiter de la plateforme ou refusées et ne pas y accéder. Il n'y a pas de juste milieu.

Deuxièmement, les rapports de pouvoir des *hackers* sont différents de ceux des citoyens numériques face aux GAFAM. Les entreprises privées continuent à exercer un rapport dominant face aux *hackers* qui utilisent leurs plateformes. Par contre, contrairement aux citoyens numériques, les *hackers* possèdent en général des compétences plus poussées en informatique, comme les membres de Crypto.Québec. Les *hackers* semblent donc moins naïfs et plus au fait du rapport dominant exercé par les GAFAM.

Troisièmement, Crypto.Québec fait aussi face au rapport dominant des entreprises privées. Par contre, en tant qu'organisme de sensibilisation en matière de vulgarisation des enjeux numériques, il cherche à s'entourer d'une communauté qui vit elle aussi cette domination. Cela porte l'organisme à adopter un rapport de pouvoir neutre et équilibré avec une communauté de citoyens numériques avec qui il souhaite échanger sur ces enjeux.

Quatrièmement, Crypto.Québec entretient un rapport de pouvoir d'égal à égal avec les médias et les autres organisations de sensibilisation avec qui il collabore. Dans le cas des médias, l'organisme amène un point de vue d'expert aux journalistes, ce qui tend à rendre la nouvelle plus compréhensible et crédible.

Lorsque Crypto.Québec s'exprime au sujet des enjeux numériques, il fait aussi face à des rapports de pouvoir multiples, variés et dispersés entre des dominants et des dominés. Le discours de l'organisme sert en quelque sorte à dire tout haut ce que les autres pensent tout bas : ce qui est caché par les entreprises privées ou non compris par les citoyens numériques. Il agit à titre de médiateur entre ces deux types de protagonistes, s'informant sur les mécanismes mis en place par le premier et fournissant au second des conseils pour pouvoir les contourner.

En effet, Crypto.Québec tend à faire la promotion de conseils et de services qui vont souvent à l'encontre des usages prescrits par les entreprises du GAFAM. Comme une forme de résistance, il questionne les usages en ligne et cherche à voir s'il y a des façons de les améliorer, de les penser différemment en fonction des usagers et non des entreprises. Le discours employé par l'organisme s'oppose à des rapports de pouvoir de manière à trouver les fuites possibles pour créer de nouveaux rapports. L'organisme transmet des astuces à sa communauté afin qu'elle puisse adopter de nouvelles pratiques à l'intérieur des usages prescrits. Les GAFAM se dotent de stratégies pour permettre aux usages prescrits de perdurer dans le temps. Ce qui constitue, en même temps, un foyer de résistance qui se doit d'être exploité par ceux qui cherchent à se défaire des usages prescrits par la mise en pratique de tactiques. Comme le rappelle la philosophe française Judith Revel dans son livre *Le vocabulaire de Foucault*, « chaque mouvement de l'un sert de point d'appui pour une contre-offensive de l'autre » (Revel, 2002 : 40). Les conseils et les services de l'organisme tendent alors à explorer les points de fuite possibles à l'intérieur du rapport de pouvoir, tout comme la tactique qui cherche des occasions à l'intérieur de la stratégie.

5.3.3.Des conseils et des services comme tactiques de détournement

Rappelons que De Certeau aborde la tactique en complémentarité avec la stratégie. De fait, les sujets de pouvoir (entreprises, gouvernements, etc.) usent de stratégies pour établir un lieu propre et imposent des types d'opérations pour que les usagers circulent à travers ce lieu dans un objectif prédéterminé (productions de données) (*op. cit.*, De Certeau, 1990 : 59). Nous observons dans le discours de Crypto.Québec que les membres profitent d'occasions pour faire face au contrôle exercé par les entreprises du GAFAM. L'organisme cherche ainsi à braconner et à détourner ce lieu propre à l'aide de tactiques qui tendent à réinventer les usages réels (pensés par les usagers et non pour les fabricants) pour permettre à la population d'adopter de meilleures habitudes en ligne.

Tout d'abord, l'organisme utilise sous forme de tactique les conseils d'experts pour atteindre le plus grand nombre de personnes à travers ses moyens de communication (émissions de baladodiffusion, interventions médias, etc.). Dans un premier exemple, nous avions soulevé dans notre problématique la possibilité pour Facebook de suivre ses usagers en dehors de sa plateforme à partir des modules de partage « J'aime » placés sur la plupart des sites Web (*op. cit.*, Roesner et coll., 2012 : 5). À cet effet, Crypto.Québec conseille d'utiliser un navigateur pour Facebook et un autre navigateur distinct pour les autres sites Web afin de détourner ce type de suivi.

Dans un second exemple, Crypto.Québec conseille l'utilisation du logiciel Tor pour naviguer sur Internet. Nous pouvons faire un parallèle avec l'exemple donné par De Certeau des employés qui font « la perruque » (*op. cit.*, De Certeau, 1990 : 43). Dans l'usine, les employés sont accusés de voler du temps et de l'argent, car ils utilisent les

machines et les biens manufacturiers « dans le but de fabriquer un objet en dehors de la production normale de l'entreprise » (Anteby, 2003). Sur le *dark web*, ceux qui utilisent Tor naviguent sur des sites non référencés dans les moteurs de recherche traditionnels, ce qui leur permet de ne pas être suivis. Pendant que des usagers fabriquent des perruques (des recherches effectuées sur Internet) dans une usine prédéterminée avec des intentions économiques (ex. : Google), nous avons, pendant ce temps, d'autres ouvriers qui fabriquent librement des perruques (des recherches anonymes) dans une salle à part (Tor).

Un troisième exemple soulevé par l'organisme est l'*obfuscation* qui consiste à obscurcir sa présence en ligne. Si au lieu de remettre des données « nettoyées »[62], les usagers en détournaient leur utilité et en réduisaient la qualité en augmentant la quantité. Nous émettons l'hypothèse que la valeur des données vendues aux annonceurs diminuerait et que les grandes entreprises de la Silicon Valley chercheraient à réinventer leur modèle d'affaires. Rappelons que les conseils de l'organisme ne sont pas sans risques. Nous avions abordé dans la problématique l'identification du graffiteur Banksy qui fut démasqué à partir d'une corrélation de données (*op. cit.*, Hauge et coll., 2016). L'organisme met en garde les usagers qui utilisent un logiciel de protection pour cacher leur identité en ligne, car ils peuvent apparaître suspects dans une foule d'individus qui n'utilisent pas ledit logiciel. Les usagers doivent alors redoubler de prudence.

Ensuite, l'organisme cherche à braconner le lieu propre en allant là où les discours des entreprises du GAFAM sont sous-représentés. Par exemple, l'organisme est souvent seul dans les médias pour faire valoir leur point de vue, et ce, sans la présence de représentant d'entreprises privées, tels Facebook ou Google. Évidemment, le Québec est un petit territoire, alors il serait étonnant de voir une

[62] Des données qui auraient été extraites, analysées et structurées grâce à des techniques de classification et d'exploration de base de données.

entreprise de la Silicon Valley envoyer un représentant pour défendre ses intérêts. Au-delà des interventions publiques, l'organisme offre des services pour se rapprocher de son public. En misant sur le contact humain, en face à face, l'organisme va encore une fois là où les entreprises privées ne se trouvent pas.

Finalement, l'organisme Crypto.Québec cherche à fournir des renseignements de base à sa communauté pour lui permettre d'avoir une meilleure vue d'ensemble de ses données et de développer un esprit critique. Nous abordions dans la pertinence de notre recherche la nécessité d'avoir une prise de conscience au sein de la société au sujet de l'utilisation des données. Cette prise de conscience est omniprésente dans le discours de Crypto.Québec qui cherche à bien des égards à informer les usagers sur l'état de leurs données. Cela se fait notamment par la promotion de la résistance : résister aux usages des fabricants et ne pas avoir peur de détourner et de changer ses « manières de faire » en ligne. Le but de cette résistance est de permettre aux usagers de « développer un esprit critique » envers les plateformes afin de comprendre pourquoi elles ont été pensées ainsi par le fabricant. Formant potentiellement des usagers plus au courant, moins indifférents et capables de remettre en question les plateformes numériques.

Nous avons des usagers qui n'ont pas d'autres choix que d'utiliser les services qui sont offerts sur le marché. Si on se soucie de sa vie privée, il faut, en tant qu'utilisateur, chercher à minimiser ses traces, mais il faut également se retourner vers les compagnies pour demander plus de pouvoir, de liberté et d'autonomie : « Ça ne doit pas peser uniquement sur les épaules de l'utilisateur, [ce n'] est pas des rapports de pouvoir qui sont équivalents » (*op. cit.*, H38).

Après avoir fait des parallèles entre le contexte du discours de Crypto.Québec et notre cadre théorique, nous poursuivons notre discussion avec notre première question de recherche – **Les pratiques mises de l'avant par Crypto.Québec s'inscrivent-elles**

comme tactique au sens indiqué par De Certeau ? –, où nous supposions l'existence de points de fuite et d'occasions pour l'organisme de s'approprier les « manières de faire ».

Dans le discours de Crypto.Québec, nous avons pu observer deux pratiques de « braconnage », les conseils et les services comme « des blocs tactiques » (*op. cit.*, Foucault, 1976 : 134-135) au sein des rapports de pouvoir exercés par les entreprises du GAFAM. Tout comme les citoyens numériques, l'organisme fait face à la supériorité de ces entreprises, ce qui le pousse à utiliser l'art du « ''faible'' afin de tirer profit du ''fort'' » (*op. cit.*, Zine, 2010 : 419). En donnant des conseils d'experts ou en offrant à sa communauté des services sur les enjeux numériques, Crypto.Québec est constamment en mouvance. Il explore toutes les directions et cherche par l'usage de tactiques à profiter des occasions, des fuites possibles « à l'intérieur du champ de vision de l'ennemi » (*op. cit.*, De Certeau, 1990 : 61). La tactique est alors une action calculée dans les fuites où le lieu propre semble absent.

Par exemple, un usager qui se dit insatisfait des conditions d'utilisation qui lui sont proposées pour accéder à une plateforme en ligne n'a pas de possibilité de s'exprimer. Il est confiné à les accepter sans les remettre en question, ou à les refuser, sans pouvoir ensuite accéder à la plateforme. Il n'y a pas de débat possible. Or, les conseils d'experts de l'organisme visent au contraire à atteindre le plus grand nombre de personnes à travers ses moyens de communication (émissions de baladodiffusion, interventions médias, etc.). L'organisme cherche à fournir une meilleure compréhension des enjeux numériques, mais surtout à provoquer des discussions, à révéler les dessous de ces plateformes et à alimenter les débats. Les conseils de Crypto.Québec visent à développer chez les usagers un esprit critique. Les conseils tendent à réveiller les usagers, les amener à se demander s'il est normal qu'autant de données soient collectées sur eux. Une application est gratuite ? Pourquoi l'est-elle ? Par qui a-t-elle été créée ? Quelles catégories de données sont recueillies ? À qui sont-

elles vendues ? Cela mène donc possiblement les usagers intéressés aux enjeux numériques à redouter l'utilisation des structures en place et l'acceptation de leurs conditions d'utilisation.

L'organisme profite également des occasions pour aller là où les entreprises du GAFAM sont sous-représentées. Alors que « les stratégies misent sur la résistance que l'établissement d'un lieu offre à l'usure du temps » (*op. cit.*, De Certeau, 1990 : 67), par exemple, les conditions d'utilisation qui donnent souvent carte blanche aux entreprises privées suite au consentement de leurs usagers, l'organisme va profiter des opportunités qui n'ont pas été prévues par les GAFAM afin de détourner leur discours. Invité à commenter dans les médias des scandales comme Facebook-Cambridge Analytica, il se sert de ces interventions pour glisser des conseils afin de minimiser les risques entourant la surveillance et la protection des données. Ces entrevues ne peuvent être prévues d'avance par les entreprises privées. Surtout, au Québec, loin des sièges sociaux des géants informatiques, Crypto.Québec se retrouve souvent seul à faire valoir son point de vue, à crédibiliser son discours face à des entreprises privées qui ne sont pas en situation de riposte.

De plus, l'organisme met en place des activités pour se rapprocher de son public, et ce, à l'extérieur des plateformes numériques. Il cherche à rencontrer sa communauté en personne pour leur donner des conseils afin d'améliorer leurs habitudes en ligne. Encore une fois, les entreprises privées se trouvent absentes des discussions et n'ont pas la possibilité de faire valoir leur point de vue durant ces activités.

En somme, nous pensons alors que les pratiques de détournement mentionnées par Crypto.Québec (conseils d'experts et offre de services) peuvent être observées comme des actes de « bricolage » qui s'inscrivent dans la tactique au sens indiqué par De Certeau. Quand De Certeau fait allusion au verbe « bricoler » dans son livre *L'invention du quotidien*, pour lui, « les usagers ''bricolent'' avec et dans l'économie

culturelle dominante les innombrables et infinitésimales métamorphoses de sa loi en celle de leurs intérêts et de leurs règles propres » (*op. cit.*, De Certeau, 1990 : XXXIX). De la même manière, Crypto.Québec circule à travers le système technique imposé par les GAFAM, à la recherche de possibilités nouvelles. Ainsi, l'organisme use de pratiques de « braconnage », de tactiques, pour détourner les manières de faire des plateformes en ligne afin de rejoindre leur mission : l'émancipation et l'avancement des libertés individuelles et collectives.

5.4. Stratégie et Crypto.Québec

Les entreprises du GAFAM possèdent un lieu propre, qu'ils ont façonné de manière stratégique : des structures complexes, lourdes et difficilement inaccessibles. Pour faire face à ce lieu institutionnalisé, Crypto.Québec doit à son tour lutter « institutionnellement » contre ce lieu propre. Ainsi, Crypto.Québec qui cherche à détourner les usages prescrits doit explorer ce système complexe pour se l'approprier, mais aussi chercher à bâtir un lieu propre. Il peut mettre en place des pratiques de détournement qui font la promotion d'usages qui n'avaient pas été pressentis par les entreprises privées. Nous pensons ici à la tactique de l'*obfuscation* mentionnée précédemment, où Crypto.Québec fournit des conseils pour obscurcir sa présence en ligne par la production de données trompeuses. Les entreprises privées n'ont sans doute pas prévu la vente de données de mauvaise qualité à leurs partenaires (ex. : régies publicitaires). Ainsi, la tactique vient affecter les rapports de pouvoir induits pour chercher à créer de nouveaux rapports de pouvoir qui contribuent à protéger la vie privée des usagers. Cependant, pour que ces pratiques de détournement puissent perdurer dans le temps, et qu'elles soient intégrées dans les habitudes du quotidien, elles doivent avoir un lieu propre et pouvoir se reproduire dans le temps. Ce lieu doit servir de base pour gérer ses relations avec une « extériorité distincte » et « capitaliser ses avantages » pour ne plus dépendre des occasions (*Ibid.*, De Certeau,

1990 : XLVI). Le discours de Crypto.Québec ne doit donc pas seulement chercher à attirer l'attention de la population, mais aussi des instances gouvernementales qui pourraient contribuer à l'instauration de nouveaux règlements en matière de vie privée en ligne. Il s'agit là de donner un caractère institutionnel, permanent et durable aux pratiques de détournement.

Comme nous rappelle De Certeau, les sujets de pouvoir usent de stratégies pour « institutionnaliser » leur lieu propre et maintenir à l'écart toute forme de résistance (*op. cit.*, Zine, 2010 : 418). Ce lieu propre institutionnalisé est tel que les entreprises du GAFAM sont devenues des puissances économiques du Web, en situation de quasi-monopole technologique, qui imposent un circuit marchand de données en fonction de leurs intérêts dans la spirale d'expansion du capitalisme. Établissant des liens serrés avec l'État et les instances gouvernementales (tel que révélé par Snowden en 2013), les GAFAM « participent au ''nouvel espace de circulation du capital''. [...] Internet est devenu une source de profit, ce n'est plus un bien public » (Sushcheva et Fontanel, 2018 : 3). Les institutions démocratiques font du surplace pendant que les intérêts privés régissent la manière dont doivent circuler les données en ligne.

À l'heure actuelle, les entreprises du GAFAM profitent de la méconnaissance de la population à propos des données et des utilisations faites à partir de celles-ci. Il ne semble donc pas y avoir d'inquiétude pour les sujets de pouvoir. Par exemple, les médias socionumériques comme Facebook demandent aux usagers d'accepter des conditions d'utilisation longues et complexes. Or, qui a la capacité de saisir clairement des conditions écrites par des juristes ? Avec peu d'options devant eux, les usagers se retrouvent donc en position d'infériorité sur ces plateformes : « c'est un choix d'utiliser l'application ou de ne pas l'utiliser » (H35).

Pour remplir sa mission, soit « l'émancipation et l'avancement des libertés individuelles et collectives » (D17), Crypto.Québec oscille entre la tactique et la stratégie pour produire un lieu propre à ses intérêts. En plus de ses tactiques de détournement (conseils d'experts, offre de services), l'organisme met en place des stratégies, soit une structure organisationnelle (conseil d'administration et conseil exécutif) qui lui permet d'accueillir de nouveaux membres, de développer de nouveaux partenariats et d'agrandir la portée de ses activités. Bref, Crypto.Québec cherche, tout comme les entreprises du GAFAM, à se donner les moyens de pouvoir ériger un lieu propre. Notamment, le fait d'établir une structure organisationnelle (conseil d'administration, conseil exécutif) lui permet de s'enregistrer en tant qu'organisme sans but lucratif. Cela lui offre un statut légal pour pouvoir exercer ses fonctions pour le bien-être de la collectivité, mais aussi la possibilité d'amasser des fonds supplémentaires (collecte de fonds) afin de faire croître ses activités.

Également, Crypto.Québec mène des actions tactiques sur deux paliers pour compléter sa mission. D'abord, l'organisme cherche à susciter l'intérêt du plus grand nombre de personnes sur les enjeux numériques. Crypto.Québec tente de vulgariser l'information pour enrichir les connaissances du public de manière à ce qu'il puisse ensuite alimenter à leur tour le débat public. Par exemple, les membres de l'organisme ont écrit un livre collectif afin de détailler « des principes de base de la sécurité numérique » et de fournir un manuel pratique à la population (D24). Si quelques individus s'opposent à l'usage des données par les géants du Web, la situation restera la même. Toutefois, si une majorité de la population est mécontente et le dit tout haut, les GAFAM pourraient reconsidérer leur modèle d'affaires en fonction des demandes des usagers. Ce faisant, des actions tactiques menées par un groupe d'individus peuvent mener à une pression sociale contre les usages prescrits par les entreprises privées. En effet, « si c'est financièrement non viable » (F12) d'utiliser les données, les entreprises du GAFAM vont reconsidérer leurs façons de faire.

Cependant, ces tactiques de détournement nécessitent l'adhésion de la population, qui est souvent volontaire. Ces tactiques risquent d'être oubliées si elles ne sont pas institutionnalisées. Par exemple, si le livre collectif venait à s'insérer dans la structure d'un cours collégial ou universitaire, nous voyons là la possibilité de faire perdurer ces pratiques dans le temps. Autre exemple, si les instances gouvernementales venaient à récupérer certains des moyens discutés dans le livre de Crypto.Québec dans la réflexion de nouveaux règlements en matière de vie privée en ligne, nous observons encore la possibilité d'assurer la pérennité de ces pratiques de détournement. Ce n'est pas en vain que Crypto.Québec s'adresse aux hautes instances pour faire valoir ses intérêts. Avec ses interventions dans les médias, la signature d'une pétition en compagnie de 83 organisations, son appui à la communauté universitaire, l'organisme cherche à attirer l'attention des gouvernements et des entreprises privées sur les enjeux de surveillance et de vie privée en ligne. Avec ces stratégies, il cherche en quelque sorte à rendre « institutionnel » un nouveau lieu propre.

Dans notre seconde question de recherche « **Crypto.Québec est-il en voie de devenir stratégique au sens indiqué par De Certeau ? Si tel est le cas, les stratégies utilisées par l'organisme peuvent-elles influencer les rapports de pouvoir du circuit marchand des mégadonnées ?** », nous pensions dans le contexte postmoderne (et plus particulièrement le mode de reproduction décisionnel-opérationnel) qu'il était encore possible pour un organisme d'utiliser des tactiques de façon stratégique pour venir rééquilibrer les rapports de force induits par les GAFAM.

Les pratiques mises en place par l'organisme se doivent d'être institutionnalisées afin d'avoir un lieu propre réfléchi pour le bien de sa communauté. C'est un retour au mode de reproduction politico-institutionnel de Freitag où l'on préconise une « production réflexive des institutions et des règles sociales » (*op. cit.*, Freitag et

Bonny, 2002 : 33). L'organisme, seul, n'a pas la capacité ou la grandeur pour forcer les entreprises privées à revoir leur modèle d'affaires. Pour ce faire, les pratiques de Crypto.Québec doivent s'élever et être portées par des acteurs sociaux dominants. En ce sens, il cherche à mobiliser une communauté d'usagers afin de forcer les entreprises à revoir leur façon de faire.

Distribuer un guide lors d'une activité ou écrire un livre se veut presque l'établissement d'un nouveau lieu propre, où l'organisme tend à rassembler l'ensemble de leurs conseils pour écrire les règles d'un nouvel espace de jeu où les usagers adoptent de meilleures habitudes en ligne. Si nous avions un système technique qui se reproduit dans le temps avec des usagers qui circulent à travers sans les remettre en question, Crypto.Québec cherche à introduire à l'intérieur de ce circuit des usagers plus informés et plus critiques des enjeux numériques. Cela peut mener, nous pensons, à la création de nouveaux rapports de pouvoir et d'une nouvelle stratégie. Crypto.Québec tente alors de postuler « un lieu susceptible d'être circonscrit comme un propre et de servir de base à une gestion de ses relations avec une extériorité distincte » (*op. cit.*, De Certeau, 1990 : 59). Ce lieu propre leur permettrait de s'opposer aux GAFAM qui représentent une extériorité distincte.

Par contre, ce lieu propre que Crypto.Québec tente d'établir n'est peut-être pas suffisant pour faire face au lieu propre des GAFAM. Bien que l'organisme travaille ardemment à faire changer les « manières de faire » de ces entreprises privées, il se peut qu'il n'arrive pas encore à se hisser suffisamment au niveau de la « stratégie ». Premièrement, nous pensons que l'organisme est peut-être, lui aussi, affecté par le contexte hyperindividualiste. En effet, l'organisme préconise une approche « individuelle » en offrant des solutions pratiques et personnalisées à sa communauté. Deuxièmement, il ne lutte peut-être pas suffisamment contre les entreprises privées et les instances gouvernementales qui les soutiennent. Il est restreint dans ses effectifs, dans le fait que ses membres agissent à titre de bénévoles, et que leur petite équipe ne

fait pas le poids face aux grandes entreprises privées qui ont un rôle dominant dans le système économique.

Deuxièmement, pour reprendre la métaphore de De Certeau à propos de la société fourmilière (*Ibid.*, 1990 : 65-66), il se peut que les entreprises privées soient perdues dans leur réussite absolue. Cela pourrait vouloir dire que les rapports de pouvoir des GAFAM sont presque totalitaires. S'il n'y a pas de rapports d'extériorité possibles, il n'y a pas non plus de tactiques ni de stratégies possibles. Ainsi, l'organisme peut se retrouver, comme les usagers, « désorbitée », où il ne semble plus y avoir de point de repère. Les GAFAM cherchent à dissimuler leur lieu propre et leur stratégie, ce qui rend difficile la possibilité pour des organismes de venir s'y opposer. Cela fait en sorte que Crypto.Québec se retrouve à lutter contre un phénomène qui n'existe pas (ou qui souhaite rester caché). Il semble alors difficile d'ériger un lieu propre s'il n'y a plus de possibilité de résister. Sans stratégie et sans tactique, nous avons affaire à un système totalitaire, où les ouvriers de la fourmilière (usagers) ne font que suivre les directives de la reine fourmi (entreprises privées).

L'organisme est peut-être en voie de devenir stratégique au sens indiqué par De Certeau, mais serait-il en mesure d'avoir un impact significatif sur les rapports de pouvoir du circuit marchand des mégadonnées ? En effet, le défi est de taille, car il faut d'abord que la stratégie de Crypto.Québec réussisse à se hisser au-dessus de la « rationalité technocratique » des GAFAM. La stratégie doit éviter d'être « désorbitée », vidée de son sens et de son objectif, et diminuée dans une société fourmilière et totalitaire. Cela nécessite également l'adhésion d'une grande communauté d'usagers prêts à vouloir s'engager à contourner les usagers prescrits par les GAFAM, mais aussi l'adhésion des instances gouvernementales, politiques et juridiques, qui pourront institutionnaliser et pérenniser les pratiques de détournement de Crypto.Québec.

Se peut-il que le nouveau livre de Crypto.Québec puisse former des individus à braconner les usages prescrits, à limiter le nombre de données recueillies, à affecter la qualité de leurs données à l'intérieur du circuit marchand ? Se peut-il que les entreprises privées qui récoltent des données de mauvaise qualité les vendent ensuite à des agences publicitaires, court-circuitent la marchandisation des données et n'atteignent plus les mêmes résultats ? Se peut-il que les entreprises privées doivent recourir à de nouvelles manières pour faire profiter leur plateforme ? Pourrions-nous voir apparaître dans un avenir rapproché des médias socionumériques comme Facebook demander à leurs usagers de payer un montant mensuel pour l'usage de la plateforme sans qu'il ait la possibilité de récolter des données en retour ? Il est à noter que le président-directeur général de l'entreprise, Marc Zuckerberg, a annoncé récemment vouloir revoir les stratégies de sa plateforme pour se concentrer davantage sur la vie privée (notamment avec les messages éphémères et chiffrés) (Zuckerberg, 2019).

Si des scandales comme Facebook-Cambridge Analytica continuent de se produire, il serait peut-être envisageable de voir Crypto.Québec élargir encore plus sa portée, influençant encore plus d'usagers à faire pression auprès des instances gouvernementales et presser les entreprises privées à revoir leurs modèles d'affaires.

CONCLUSION

Avec les révélations d'Edward Snowden sur la NSA qui surveille et capte les données des usagers sur les GAFAM, les cartes de crédit avec des données anonymes qui peuvent être révélatrices de l'identité ou encore, plus récemment, le scandale de Facebook-Cambridge Analytica sur un usage non autorisé et non approprié de données personnelles de millions d'usagers, nous sommes conscient que les risques d'identification et de surveillance sont bien réels à l'ère des mégadonnées.

Notre projet de recherche visait notamment à explorer les différentes tactiques utilisées par un organisme de sensibilisation au Québec intéressé par l'actualité numérique (Crypto.Québec) afin de voir s'il existe des moyens à notre échelle pour s'opposer à la stratégie des GAFAM. Dans notre problématique, nous avions abordé le contexte des mégadonnées, soulevé des enjeux importants quant à la vie privée et la collecte des données, mais aussi observé les technologies numériques qui laissent entrevoir un circuit marchand. Nous avions également abordé dans notre cadre théorique le mode de reproduction décisionnel-opérationnel de Freitag, la gouvernementalité et les rapports de pouvoir de Foucault, et la stratégie et la tactique de De Certeau. Ceci nous a ensuite conduit à une analyse critique du discours de Crypto.Québec, un organisme qui alimente les débats contemporains sur la sécurité informatique et qui traite des mégadonnées, de l'identification et de la surveillance par le biais de leurs plateformes et de leurs services. Notre corpus, composé notamment de leurs balados et de leurs interventions médiatiques, nous a permis de prendre conscience de la domination exercée par les entreprises du GAFAM sur les usagers, l'un des principaux objectifs de l'analyse critique du discours (*op. cit.*,

Fairclough, 1989 : 3). Cet exercice nous a permis de nous plonger au cœur même de l'univers de Crypto.Québec et de nous placer dans la perspective du public qui le suit. Si le contenu de leurs propos porte notamment sur la surveillance, la vie privée et le *hacking*, nous nous sommes senti par moment comme un espion qui tentait de collecter tous les renseignements disponibles sur l'organisme… comme si notre démarche de recherche nous faisait penser aux GAFAM qui surveillent et extraient au quotidien les données de ses usagers ! Nous avons été surpris de la quantité de données que nous pouvions récupérer sur une période d'un an, mais évidemment, notre corpus est restreint par rapport à l'information que pourrait amasser, par exemple, un média socionumérique quelconque sur Crypto.Québec. Bien que nous ayons accès à leurs publications, Facebook peut, de son côté, suivre dans l'ombre les gestionnaires de la page Facebook de Crypto.Québec (heures passées en ligne, messages privés envoyés, etc.) qui sont liés à des comptes Facebook personnels des membres, ce qui fait en sorte que Facebook détient sans doute plus de données que nous sur l'organisme.

Pour revenir à notre question générale de recherche « **Dans un tel contexte, comment Crypto.Québec peut-il affecter, modifier ou détourner les rapports de pouvoir du circuit marchand des mégadonnées induits par les GAFAM ?** », nous cherchions à déterminer, dans le contexte d'identification ou de surveillance à l'ère des mégadonnées, s'il était possible pour Crypto.Québec de résister aux GAFAM, de détourner à travers leurs pratiques les usages prescrits de façon à fournir à sa communauté des astuces pour protéger sa vie privée en ligne et éventuellement s'opposer aux entreprises privées. À la lumière du discours de Crypto.Québec, nous avons vu que l'organisme se sert de tactiques de détournement (conseils d'experts, offre de services) et d'occasions pour faire face au contrôle exercé par les géants technologiques. L'organisme invite les usagers à réinventer les usages prescrits et pensés par les fabricants afin d'adopter de meilleures habitudes en ligne. Également, en suscitant l'intérêt des usagers et en collaborant avec leurs partenaires (médias,

universitaires, organismes similaires, etc.), nous avons appris que Crypto.Québec utilise l'art du faible dans le territoire du plus fort. L'organisme se sert de la tactique de manière à profiter de toutes les fuites possibles qui se trouvent à l'intérieur du champ de l'ennemi (entreprises GAFAM).

Bien que l'organisme doive composer avec les réalités et défis de la population – sa faible compréhension des données, son sentiment d'infériorité à l'égard de grandes organisations et sa résiliation sur l'urgence d'agir – nous pensons, dans le contexte actuel du circuit marchand des mégadonnées (Ouellet et coll., 2016), qu'il est encore possible pour l'organisme d'encourager les usagers à contourner les entreprises du GAFAM, en leur partageant de nouvelles « manières de faire » pour renforcer leur vie privée en ligne, tout en développant leur esprit critique. Le but ultime étant de forcer les entreprises privées à changer les modèles d'affaires de leurs plateformes. Cependant, il faut un grand nombre de personnes pour effectuer une pression sociale et pour arriver à des changements significatifs auprès de ces entreprises selon Crypto.Québec. Il faut également le soutien de l'État pour mettre en place des règlements tenant compte des pratiques de détournement de l'organisme, ce qui relèverait de la stratégie et de l'établissement d'un lieu propre.

Par contre, comme nous l'avons vu dans le mode de reproduction décisionnel-opérationnel de Freitag, nous assistons à l'occultation politique par l'expansion du capitalisme. Les GAFAM, qui font passer leur profit avant tout, se perdent dans leur réussite absolue. Elles cherchent à camoufler le lieu propre, la stratégie et la structure qui encadrent leurs manières de faire. Cela amène un défi de taille à l'organisme qui peut se retrouver parfois, tout comme sa communauté, « désorbité » ne sachant plus à qui s'opposer. Pour lutter contre le lieu propre institutionnel de ces entreprises privées, Crypto.Québec ne doit pas seulement penser à promouvoir des solutions individuelles auprès de sa communauté. Il doit surtout chercher à

« institutionnaliser » et à rendre ses pratiques permanentes de façon à ce qu'il y ait un changement de conscience dans la protection de la vie privée en ligne.

L'espoir est à portée de main. Les évènements qui compromettent les données personnelles des usagers se sont multipliés récemment (Spectre, Meltdown[63], Facebook-Cambridge Analytica, etc.) et ont été révélés au grand jour. Si la tendance se maintient, ces évènements pourraient sensibiliser toujours davantage la population à l'égard de leurs données. Ce n'est pas en vain que Crypto.Québec a été appelé à commenter l'actualité médiatique dans la dernière année. Sa présence accrue dans les médias lui a permis d'agrandir son équipe, d'étendre la portée de sa mission de Montréal à l'échelle de toute la province, rejoignant ainsi une plus grande portion du grand public, mais également les gouvernements et les entreprises privées. Tandis que les GAFAM profitent de la méconnaissance de leurs usagers avec la mise en place de stratégies qui les invitent à profiter des fonctionnalités de ces plateformes sans les questionner, Crypto.Québec mise plutôt sur le partage des connaissances. L'organisme veille à informer son public sur les usages prescrits, leur fournir de nouvelles « manières de faire » pour contourner le circuit marchand des plateformes en ligne et finalement adopter un point de vue critique sur l'usage de leurs données.

Les appareils technologiques de plus en plus personnalisés misent davantage sur l'individu que sur le vivre-ensemble et rappelons-le, « [finissent] par s'imposer comme la forme la plus évidente, la plus contraignante de la réalité » (*op. cit.*, Freitag et Bonny, 2002 : 111). Dans ce contexte, nous pouvons nous demander si les stratégies mises en place par Crypto.Québec, notamment la stratégie de prôner de nouvelles pratiques individuelles au sein d'une société essentiellement hyperindividualiste et pragmatique est viable à long terme. Cette stratégie peut

[63] Dévoilées en janvier 2018, les deux failles de sécurité, Spectre et Meltdown, auraient permis à des pirates de s'emparer d'informations confidentielles contenues dans les ordinateurs (codes de chiffrage, mots de passe, etc.) (Vallée, 2018).

néanmoins réveiller les usagers quant aux conséquences possibles de la collecte massive et de la marchandisation de leurs données personnelles. Nous pensons que cela peut les inciter à agir, par exemple, en demandant une intervention du gouvernement pour forcer les GAFAM à revoir leur modèle économique pour le bien de la collectivité.

Enfin, nous pensons que notre recherche entraînera un savoir socialement pertinent et une prise de conscience pour le lecteur-usager soucieux de la captation de ses données numériques qui s'effectue à l'écart par des entités tierces. Sur le plan du savoir scientifique, il fut pertinent d'approcher un organisme québécois qui s'intéresse comme nous aux enjeux de surveillance et d'identification. Cela nous a permis d'approfondir nos théories avec un point de vue d'expert dans ce domaine et d'obtenir des exemples concrets. Également, la réactualisation de la théorie de la stratégie et de la tactique de De Certeau, dans le contexte actuel des mégadonnées, nous a aidé à identifier les occasions pour l'organisme de contourner les usages prescrits par les GAFAM.

Bien que nous cherchions à rendre compte des stratégies et tactiques d'une organisation québécoise, nous sommes conscient que Crypto.Québec n'est pas représentatif de tous les organismes traitant des enjeux de sécurité informatique et que les membres de l'organisme communiquent avec une certaine partie de la population des usagers au Québec. De plus, il ne faut pas perdre de vue que les propos recueillis sont dans un contexte où les membres de l'organisme adoptent un discours engagé et marqué par des intérêts et des valeurs propres à leur organisation. Sinon, nous n'avons pas le point de vue des entreprises du GAFAM, qui sont situées pour la plupart à l'extérieur du pays, ce qui aurait pu apporter certaines nuances au discours de Crypto.Québec. De plus, la route à suivre, de la tactique à la stratégie, est un défi de taille. L'organisme cherche à susciter l'intérêt des usagers, mais c'est loin d'être gagné, car les plateformes développées par les géants technologiques sont

ancrées de plus en plus dans les habitudes de leur quotidien. L'organisme a encore besoin de beaucoup de temps pour sensibiliser les usagers à adopter de nouvelles habitudes en ligne et se doit de continuer son travail tout en étendant la portée de ses activités.

Ceci étant dit, si des évènements comme le scandale Facebook-Cambridge Analytica surviennent davantage, cela facilitera le travail de l'organisme. Plus les usagers seront inquiets à l'égard de leurs données, plus nous pensons que Crypto.Québec pourra intervenir et leur montrer comment faire pour réinventer leurs usages par rapport aux GAFAM. Les usagers plus conscientisés pourraient alors s'unir pour se révolter, demander aux gouvernements d'intervenir et forcer les géants du Web à revoir leurs modèles d'affaires.

D'ailleurs, à partir du moment où nous avons commencé à écrire notre mémoire sur les enjeux numériques de surveillance et d'identification, nous avons pu assister à de nombreux évènements compromettant la sécurité des données, notamment les failles informatiques de Spectre et Meltdown, le fait que les usagers des appareils Google sont suivis malgré la désactivation du paramètre de géolocalisation (Ici Radio-Canada, 2018), et ce n'est que le début. Il est fort probable que d'autres évènements de ce type surviennent dans les prochaines années. Les usages du Web sont en constante évolution et nous produisons de plus en plus de données ; nous n'avons qu'à penser à l'arrivée de l'Internet des objets dans les maisons. Ceci devient alors plus alarmant pour les usagers victimes de failles informatiques ou qui ne sont pas conscients de leurs données produites, cédées aux entreprises privées. Somme toute, il n'est jamais trop tard pour s'opposer et réinventer nos « manières de faire » en ligne. Les voix de Crypto.Québec et des usagers s'élèvent graduellement. Est-ce suffisant ? Seuls le temps, les choix et les actions que nous ferons en tant qu'usagers nous le diront.

En guise d'ouverture, nous revenons sur le livre collectif que Crypto.Québec a écrit et sorti en septembre 2018, après le recensement de nos données pour cette recherche. Ayant pour titre *On vous voit : Comment déjouer les malveillants sur Internet*, ce guide pratique apporte un complément d'information sur le discours relevé. L'organisme revient sur l'importance que son équipe a dans l'analyse des enjeux numériques, notamment les formes de surveillance et de collectes de données effectuées par les GAFAM. Crypto.Québec « doit se positionner dans l'espace public afin de les observer, de les analyser et les vulgariser pour une grande partie de la population » (Crypto.Québec, 2018 : 12). Un désir de partager des connaissances avec une plus grande partie de la population qui se retrouve présentement désavantagée dans le contexte actuel.

De plus, l'organisme traite d'un chapitre intéressant sur l'ingénierie sociale et les vulnérabilités de l'être humain. En fait, l'ingénierie sociale est définie comme étant « l'art de comprendre les failles psychologiques de l'humain afin de mieux le manipuler » (Crypto.Québec, 2018 : 47). Cet art est de plus en plus utilisé par des *hackers* de types criminels afin d'influencer le comportement des individus en ligne en vue de les pirater ou de les attaquer (ex. : voler leur identité en ligne). L'organisme mentionne l'importance de se mettre dans la peau de ces *hackers* qui attaquent pour bien comprendre l'ingénierie sociale, soit « dans un premier temps, une analyse minutieuse de la situation afin de procéder, dans un deuxième temps à l'attaque qui permettra, si l'opération réussit, la manipulation de la cible » (*Ibid.*, 2018 : 48). Nous y voyons un rapprochement à faire avec la tactique employée par l'organisme pour former les usagers en ligne afin de contourner les usages prescrits par les plateformes en ligne. Tout comme l'attaquant, Crypto.Québec cherche à se mettre dans la peau de ceux qui récoltent des données de manière à vulgariser et à fournir des connaissances à sa communauté, afin de les influencer à adopter de nouvelles « manières de faire » à l'intérieur du territoire de l'ennemi (plateformes en ligne des GAFAM).

Enfin, Crypto.Québec illustre dans la conclusion de son livre un parallèle sur le mouvement environnemental et la lutte contre le changement climatique. Comme quoi les actions menées individuellement peuvent potentiellement mener à des changements collectifs. Pour s'attaquer aux enjeux numériques et arriver à influencer les entreprises privées à revoir leurs modèles d'affaires, « le changement de conscience [doit passer], entre autres, par l'adoption de meilleures pratiques à l'échelle individuelle » (*Ibid.*, 2018 : 135). Du côté de l'environnement, le changement d'un seul individu ne peut avoir un impact significatif. Or, si tout un chacun améliore leur posture numérique et sont de plus en conscients des usages prescrits par les entreprises du GAFAM, ils pourront selon l'organisme, « contribuer à un changement de culture à l'échelle collective » (*Ibid.*, 2018 : 135).

Sur une note plus personnelle, nous avons parcouru beaucoup de chemin au fil de l'écriture de ce mémoire, mais surtout développé une prise de conscience. Plus nous lisions sur les enjeux numériques, plus nous en apprenions sur l'état de nos données. Cela nous a mené à nous écarter tranquillement de l'usage de ces plateformes. Nous avons pratiquement cessé de créer du contenu sur les médias socionumériques tels Facebook, Instagram, Twitter et LinkedIn. Nous avons commencé à utiliser sur une base quotidienne DuckDuckGo, un moteur de recherche qui ne nous espionne pas ainsi que Brave, un navigateur Web qui tend à protéger la vie privée. Nous avons fermé nos paramètres de géolocalisation et Bluetooth sur notre téléphone intelligent lorsqu'ils n'étaient pas nécessaires. Nous avons payé pour télécharger des logiciels au lieu de remettre nos données en échange d'applications gratuites. Nous nous sommes déconnecté, la plupart du temps, des appareils technologiques et des écrans pour profiter de la vie sans produire de données. Néanmoins, aux fins de notre recherche, nous sommes resté connecté sur Facebook sans y participer, adoptant un comportement de badaudage (*lurking*), soit un « terme péjoratif commun pour ceux qui sont présents dans les espaces publics en ligne, mais ne parlent pas en

évidence[64] » (Crawford, 2009 : 526). Il n'est pas dit dans les prochaines années que nous pourrions éventuellement nous déconnecter de ces plateformes au profit de nouveaux médias socionumériques qui seront plus respectueux de la vie privée de ses usagers et où nous aurons également la certitude que les données resteront dans notre pays avec nos valeurs et non dans des centres de données hébergés dans d'autres pays, sans connaître leurs motivations.

[64] Traduction libre

ANNEXE 1

TABLEAU DE BORD DE GOOGLE ANALYTICS

ANNEXE 2

CORPUS DES DOCUMENTS SÉLECTIONNÉS

#	Titre du document	Type de communication	Source	Support	Locuteur	Date de diffusion
1	40 : Questions du public, les IMSI catchers de GRC et la National Geospatial-Intelligence Agency	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu, Sophie Thériault	2017-03-22
2	43 : Une sécurité des données déficiente au SPVM, ShadowBrokers qui publie des outils de la NSA et le démantèlement du botnet Kelihos	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Jean-Philippe Décarie-Mathieu	2017-04-12
3	45 : Tracking Bluetooth, reconnaissance automatique des plaques de véhicules à Montréal et un NIP sur votre SIMM	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Sophie Thériault	2017-05-03
4	49 : Les politiques de modération de Facebook, la surveillance des militants à Standing Rock et l'origine de Shadow Brokers	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Sophie Thériault	2017-05-31
5	51 : Spécial questions et réponses en direct	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu, Luc Lefebvre	2017-06-14

6	53 : Petya, la Chambre des communes anglaise compromise et un porte-avion roulant sous Windows XP	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu	2017-06-28
7	54 : Les PMEs et les attaques informatiques, wangiri et un coup de filet de la police sur le darknet	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu, Anne-Sophie Letellier	2017-07-05
8	59 : L'arrestation de MalwareTech, la sécurité des systèmes de votation et le danger de certains VPNs « gratuits »	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu	2017-08-09
9	76 : Des conseils de sécurité en famille pour le temps de Fêtes, Messenger Kids et le gold farming au Venezuela	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier, Sophie Thériault	2017-12-06
10	79 : Meltdown & Spectre, 34c3 et les photos d'enfants sur les réseaux sociaux	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Sophie Thériault	2018-01-04
11	81 : Une autre fuite chez Bell, des montres qui en savent trop et un front des télécoms canadiennes contre la neutralité du Net	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Jean-Philippe Décarie-Mathieu, Luc Lefebvre	2018-01-31
12	82 : L'attribution et la Russie (encore), la géolocalisation sans GPS et des lunettes intelligentes orwelliennes en Chine	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu	2018-02-07

13	86 : Spécial intelligence artificielle avec Samuel St-Pierre	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu	2018-03-08
14	87 : La valeur d'une identité numérique, les tendances émergentes en cybercriminalité et comment contourner une cage de Faraday	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Jean-Philippe Décarie-Mathieu	2018-03-20
15	89 : Des cartes d'accès d'hôtels compromises, le programme AARDVARK et la saisie de AnonIB	Émission de baladodiffusion	*Les chiens de garde* (Crypto.Québec)	Baladodiffusion	Geneviève Lajeunesse, Anne-Sophie Letellier	2018-04-26
16	Le «Dark Net» (TOR) et vous. Pourquoi et comment y accéder.	Page Web	Web à Québec	Site Web		2017-04-06
17	Crypto.Québec met en place son conseil d'administration et son comité exécutif	Article	Crypto.Québec	Site Web	Anne-Sophie Letellier, Sophie Thériault	2017-04-28
18	Ce qu'il faut retenir de #MacronLeaks	Article	Crypto.Québec	Site Web	Jessie Wala Ahmad	2017-05-18
19	Ce qu'il faut retenir de #WannaCry	Article	Crypto.Québec	Site Web	Jessie Wala Ahmad	2017-06-06

20	Crypto.Brunch	Publication Facebook	Facebook	Média socionumérique		2017-06-18
21	Film Risk de Laura Poitras	Publication Facebook	Facebook	Média socionumérique		2017-06-28
22	Crypto.Québec joint sa voix à une coalition demandant aux "Five Eyes" de respecter le chiffrement des communications	Article	Crypto.Québec	Site Web	Anne-Sophie Letellier	2017-07-03
23	L'état de la surveillance de masse en 2017, FACIL	Page Web	Facil	Site Web		2017-08-15
24	Crypto.Québec, trois années plus tard…!	Article	Crypto.Québec	Site Web		2018-03-11
25	Exposition Chambre de verre, UQAM	Article	Crypto.Québec	Site Web		2018-03-26
26	Les ateliers des spécialistes de Crypto.Québec	Page Web	UQAM	Site Web		2018-03-26

27	Le dark web, c'est quoi? 5 questions pour éclaircir cet univers mystérieux	Intervention publique	Journal de Montréal	Site Web / Journal	Jean-Philippe Décarie-Mathieu	2017-07-06
28	Repérer ses amis en temps réel : le nouvel outil de Snapchat va-t-il trop loin?	Intervention publique	Ici Radio-Canada	Radio	Geneviève Lajeunesse	2017-07-10
29	8 outils pour protéger votre vie privée	Intervention publique	Protégez-vous	Site Web / Magazine	Geneviève Lajeunesse	2017-08-07
30	Comment utiliser son téléphone en voyage sans se ruiner	Intervention publique	Les Affaires	Site Web / Magazine	Geneviève Lajeunesse	2017-09-07
31	Gare aux cyberattaques : conseils pour se protéger	Intervention publique	TVA (*Salut Bonjour*)	Télévision	Geneviève Lajeunesse	2018-01-05
32	Big Brother nous surveille-t-il	Intervention publique	Journal de Montréal	Site Web / Journal		2018-02-16
33	Ciel, mes données!	Intervention publique	La Presse	Site Web / Journal	Luc Lefebvre	2018-03-07

34	5 conseils pour mieux protéger vos données personnelles en ligne	Intervention publique	Ici Radio-Canada	Site Web	Geneviève Lajeunesse	2018-03-13
35	La sécurité de vos données	Intervention publique	CKOI 96,9 FM	Radio	Anne-Sophie Letellier	2018-03-14
36	L'intelligence artificielle	Intervention publique	TV5 Monde (*60 jours d'intelligence artificielle*)	Télévision	Geneviève Lajeunesse	2018-03-14
37	Facebook dans la tourmente : l'utilisation des données de 50 millions d'utilisateurs fait beaucoup de bruit.	Intervention publique	Ici Radio Canada (*En direct avec Patrice Roy*)	Télévision	Jean-Philippe Décarie-Mathieu	2018-03-20
38	Facebook est dans la tourmente depuis les révélations concernant la firme Cambridge Analytica, qui aurait collecté les données personnelles de 50 millions d'utilisateurs du réseau social.	Intervention publique	Ici Radio-Canada (*La Sphère*)	Site Web	Anne-Sophie Letellier	2018-03-20
39	CBC Montreal Radio Noon host Shawn Apel wants to know are you thinking of quitting Facebook in light of the alleged privacy breach?	Intervention publique	CBC Montreal (*CBC Montreal Radio Noon*)	Radio	Geneviève Lajeunesse	2018-03-22
40	Comment faire pour protéger nos données personnelles en ligne	Intervention publique	Urbania	Vidéo	Anne-Sophie Letellier	2018-03-30

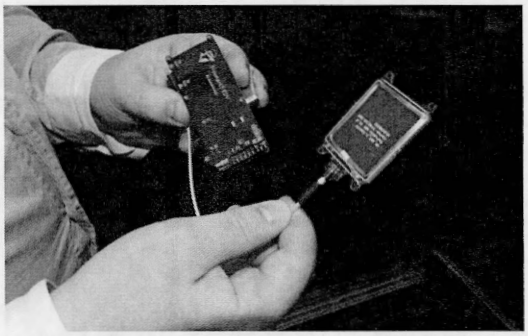
41	Trois conseils pour sexter de façon plus sécuritaire	Intervention publique	Ici Radio-Canada	Site Web	Geneviève Lajeunesse, Anne-Sophie Letellier	2018-03-31
42	Le cyberespionnage	Intervention publique	Ici Radio-Canada (*La route des 20*)	Radio	Geneviève Lajeunesse	2018-04-20
43	Données personnelles en ligne : on vous suit à la trace	Intervention publique	Ici Radio-Canada (*Tout le monde en parle*)	Télévision	Luc Lefebvre	2018-03-11

ANNEXE 3

PAGE WEB D'UNE ÉMISSION DE *LES CHIENS DE GARDE*

Les Chiens de garde #89 – Des cartes d'accès d'hôtels compromises, le programme AARDVARK et la saisie de AnonIB

Afficher tous les articles par Jean-Philippe Décarie-Mathieu • 29 avril 2018



La 89e émission des Chiens de garde, le podcast de Crypto.Québec sur la sécurité, la vie privée et la surveillance, est en ligne. L'épisode a été enregistré le jeudi 26 avril 2018.

00:00

Type de fichier : OGG / MP3 – Taille : 47,31MB – Durée : 30:46 m (215 kbps 44100 Hz)

Notes de l'émission

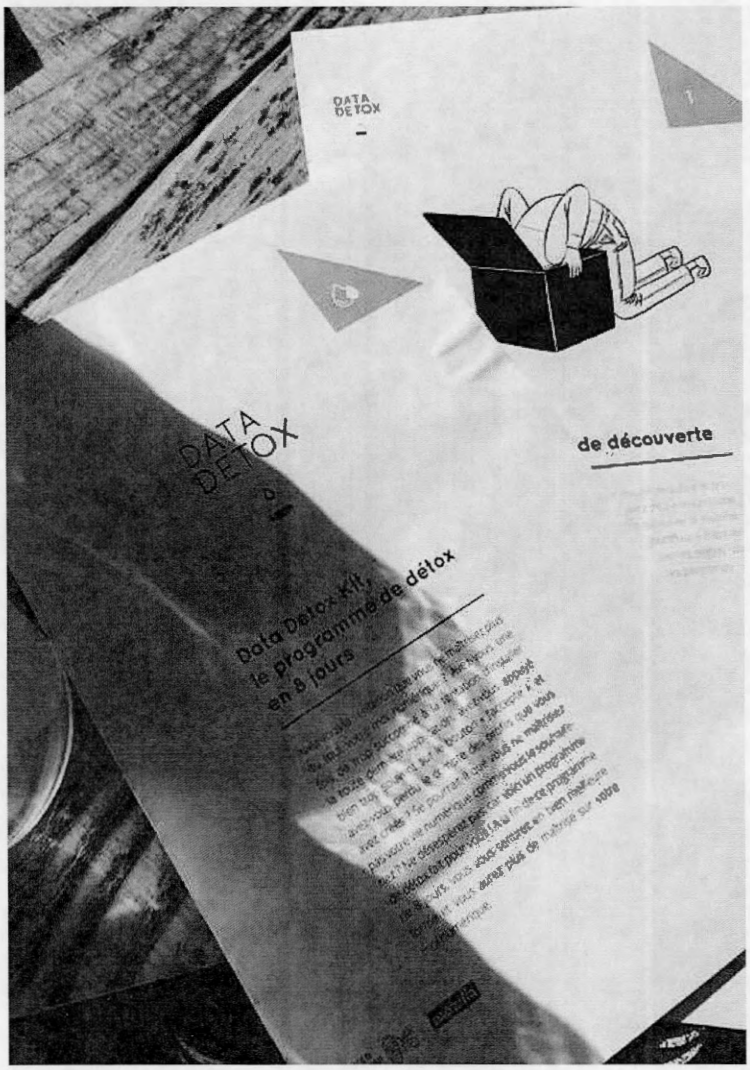
- Annonces:
  - De retour! et avec quelques changements...
  - northsec, rightscon – c'est maintenant, si vous voulez des billets!
  - Code for Canada recrute.
- Hacking:
  - Joy Reid et les hackers qui voyagent dans le temps – une démonstration par l'exemple de la nécessité de sites comme archive.org et archive.today...
  - Les cartes d'accès ASSA ABLOY utilisées dans des milliers d'hôtels compromises.
  - Do Not Disturb – pour voir qui utilise votre mac en votre absence (quel est le mode de menace?)
- Surveillance:
  - "Terreur sans idéologie" et redéfinition des menaces à la population – le cas Minassian.
  - AARDVARK, le programme de transfert de technologies du Pentagone et les manifestants pacifiques.
  - Inde et vie privée : dérapages au niveau de la divulgation des informations bancaires.
- Vie privée:
  - Anon-IB saisi par les autorités néerlandaises, poussant le phénomène du revenge porn dans le maquis.
  - Ray Ozzie et un schème à clé en compte séquestre pour "en finir avec la guerre du chiffrement"... ça ne fonctionne pas.
  - Pendant ce temps, on trouve une Graykey à découvert sur Shodan.
  - Des millions d'apps laissent fuiter des informations personnelles par le biais de l'intégration des régies publicitaires – thatoneprivacysite pour faire un bon choix niveau VPN.

Équipe

- Animation : Geneviève Lajeunesse

ANNEXE 4

GUIDE DE DÉTOX EN 8 JOURS



BIBLIOGRAPHIE

Adesias (2013, 15 juillet). *Si c'est gratuit, vous êtes le produit.* [Vidéo]. Récupéré de https://www.youtube.com/watch?time_continue=19&v=8vLSf1i4E7A

AdNauseam (2017). AdNauseam banned from the Google Web Store. Récupéré de https://adnauseam.io/free-adnauseam.html

Andrieu, B. (s. d.). CORPS - Cultes du corps. *Encyclopædia Universalis*. Récupéré de http://www.universalis.fr/encyclopedie/corps-cultes-du-corps/

Anteby, M. (2003). La « perruque » en usine : approche d'une pratique marginale, illégale et fuyante. *Sociologie du travail*, *45*(4), 453-471.

Apple (2016). About Face ID advanced technology. Récupéré de https://support.apple.com/en-ca/HT208108

Arpin-Simonetti, E. (2015). Contrôle social 2.0. *Relations*, *776*, 12-13.

Baillargeon, S. (2009). Michel Freitag 1935-2009 - Mort d'un géant de la sociologie. *Le Devoir*. Récupéré de http://www.ledevoir.com/societe/actualites-en societe/277190/michel-freitag-1935-2009-mort-d-un-geant-de-la-sociologie

Barocas, S. et Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75.

Bearman, J. (2015). The Untold Story of Silk Road, Part 2: The Fall. *Wired, 23*(5), 90–118.

Beaupré, M. (2001). La perte de la transcendance dans la société postmoderne : Étude critique des œuvres de M. Gauchet, M. Freitag et G. Lipovetsky.

Biehn, N. (2013). The missing Vs in big data: viability and value. *Wired*. Récupéré de http://www.wired.com/insights/2013/05/the-missing-vs-in-big-data viability-and-value

Birnbaum, P. (1975). *La fin du politique*. Paris : Le Seuil.

Bonenfant, M., Mondoux, A., Ménard, M. et Ouellet, M. (2015). Big Data, médiation symbolique et gouvernementalité. Dans *Big Data-Open Data : Quelles valeurs? Quels enjeux?* (31-41). De Boeck Supérieur.

Boren, Z. D. (2014). There are officially more mobile devices than people in the world. *The Independent*. Récupéré de https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

Brave (2018). Récupéré de https://brave.com/

Brunton, F. et Nissenbaum, H. (2015). *A User's Guide for Privacy and Protest*. Cambridge: The MIT Press.

Chavanel, S. (s. d.). Fiche de lectures de M. de Certeau, *L'invention du quotidien. 1. Arts de faire*, Gallimard, 1990. *Observatoire des médias sociaux en relations publiques*. Récupéré de http://www.omsrp.com.ulaval.ca/recherches-et publications/fiches-de-lecture/linvention-du-quotidien/

Citot, V. (2004). Les temps hypermodernes, de Gilles Lipovetsky. *Le philosophoire*, (1), 184-188.

CNRTL (s. d.). Appropriation. Récupéré de http://www.cnrtl.fr/definition/appropriation

CNRTL (s. d.). Braconner. Récupéré de http://www.cnrtl.fr/definition/braconner

CNRTL (s. d.). Idéologie. Récupéré de http://www.cnrtl.fr/etymologie/idéologie

CNRTL (s. d.). Institutionnaliser. Récupéré de http://www.cnrtl.fr/definition/institutionnaliser

CNRTL (s. d.). Modernisme. Récupéré de http://www.cnrtl.fr/definition/modernisme

CNRTL (s. d.). Octet. Récupéré de http://www.cnrtl.fr/definition/octet

CNRTL (s. d.). Passif. Récupéré de http://www.cnrtl.fr/definition/passif

CNRTL (s.d.). Personnalisé. Récupéré de http://www.cnrtl.fr/definition/personnalisé

CNRTL (s. d.). Stratégie. Récupéré de http://www.cnrtl.fr/etymologie/stratégie

CNRTL (s. d.). Tactique. Récupéré de http://www.cnrtl.fr/etymologie/tactique

Commissariat à la protection de la vie privée du Canada (2014). *Convergence des mégadonnées et du droit*. Récupéré de https://www.priv.gc.ca/fr/nouvelles du-commissariat/allocutions/2014/sp-d_20141017_pk/?wbdisable=true

Commissariat à la protection de la vie privée du Canada (2018). Dix conseils à suivre pour protéger vos renseignements personnels. Récupéré de https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/votre-droit-a-la-vie-privee/02_05_d_64_tips/

Conseil de l'Europe. Bureau de comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. (2016). Des données et des hommes : Droits et libertés fondamentaux dans un monde de données massives. Strasbourg : Rouvroy, A. Récupéré de http://www.academia.edu/15730565/des_données_et_des_hommes._droits_et _libertés_fondamentaux_dans_un_monde_de_données_massives

Crawford, K. (2009). Following you: Disciplines of listening in social media. *Continuum*, *23*(4), 525-535.

Crypto.Québec (2018). À propos. Récupéré de https://crypto.quebec/a-propos/

Crypto.Québec (2018). Services. Récupéré de https://crypto.quebec/services/

De Certeau, M. (1990). *L'invention du quotidien. 1. Arts de faire*. Paris : Gallimard.

De Filippi, P. (2016). Gouvernance algorithmique : Vie privée et autonomie individuelle à l'ère des Big Data. *Open Data & Data Protection : Nouveaux défis pour la vie privée*.

DuckDuckGo (2018). Récupéré de https://duckduckgo.com/

Eckert, S. et Dewes, A. (2017, 20 octobre). DEF CON 25: Dark Data. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=1nvYGi7-Lxo

Data Detox Kit (2017). Récupéré de https://datadetox.myshadow.org/fr/detox

De Hert, P. J. A. et Bellanova, R. (2008). La protection des données d'un point de vue transatlantique : l'UE et les USA sur la voie d'un accord international relatif à la protection des données? *European Parliament*. Récupéré de http://www.narcis.nl/publication/RecordID/oai:tilburguniversity.edu:publicati ons%2F1afdb0ff-0b97-46bb-9a7e-2fc6dd97f08e

De Montjoye, Y. A., Radaelli, L. et Singh, V. K. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536-539. doi: 10.1126/science.1256297

Diebold, F. X. (2012). A Personal Perspective on the Origin (s) and Development of 'Big Data': The Phenomenon, the Term, and the Discipline. *Social Science Research Network*. doi: 10.2139/ssrn.2202843

El Emam, K., Buckeridge, D., Tamblyn, R., Neisa, A., Jonker, E. et Verma, A. (2011). The re-identification risk of Canadians from longitudinal demographics. *BMC medical informatics and decision making*, *11*(1), 46.

Facebook (2018). Conditions d'utilisation. Récupéré de https://www.facebook.com/legal/terms/update

Favre, P. (1975). [Compte rendu du livre *La fin du politique*, par P. Birnbaum Pierre]. *Revue française de sociologie*, *16* (4). 564-566.

Fairclough, N. (1995). *Critical discourse analysis: The critical study of language*. Routledge.

Fairclough, N. (1989). *Language and Power*. London: Longman Publishers.

Filion, G. (2010). *La critique de l'historicité de Michel Freitag: Pour une réaffirmation de la valeur du monde* [Thèse de doctorat]. Université d'Ottawa.

Filion, J. F. et Freitag, M. (2006). *Sociologie dialectique : introduction à l'œuvre de Michel Freitag*. Montréal : Éditions Nota bene.

Foucault, M. (1972). Seconde préface pour la réédition *d'Histoire de la folie à l'âge classique*. Récupéré de https://foucault.info/documents/foucault.prefaceHistoireFolie.fr/

Foucault, M. (1975). *Surveiller et punir. Naissance de la prison*. Paris : Éditions Gallimard.

Foucault, M. (1976). *L'histoire de la Sexualité I. La volonté du savoir*. Paris : Gallimard.

Foucault, M. (1977). *Dits et Écrits II*. Paris : Gallimard.

Foucault, M. (1981, 7 mai). *Michel Foucault à l'Université Catholique de Louvain.* [Vidéo]. Récupéré de https://www.youtube.com/watch?v=132QZ_C3ovs

Foucault, M. (1994). *Dits et Écrits*, 1954-1988, volume 3, 1976-1979. Paris : Gallimard.

Freitag, M. et Bonny, Y. (2002). *L'oubli de la société : pour une théorie critique de la postmodernité*. Québec : Presses Université Laval.

Galinon-Mélénec, B. et Zlitni, S. (2013). L'Homme-trace, producteur de traces numériques. Dans *Traces numériques, de la production à l'interprétation, CNRS éditions*, 7-19, CNRS Alpha.

Gambier, Y. (2009). Stratégies et tactiques en traduction et interprétation. Dans *Efforts and Models in Interpreting and Translation Research–A Tribute to Daniel Gile*, 63-82.

Gendreau-B., G. (2009). *La crise des sciences chez Edmund Husserl et Michel Freitag* [Mémoire de maîtrise]. Université du Québec à Montréal. Récupéré de https://archipel.uqam.ca/2956/

Giles, M. (2018). The Cambridge Analytica affair reveals Facebook's "Transparency Paradox". *MIT Technology Review*. Récupéré de https://www.technologyreview.com/s/610577/the-cambridge-analytica-affair-reveals-facebooks-transparency-paradox/

Google Analytics (2017, 9 juin). *Audience reports overview*. [Vidéo]. Récupéré de https://www.youtube.com/watch?v=Bsc_7WEcgRE&list=PLI5YfMzCfRtZU5Qwzx57HjmZyNE2o5YDN&index=7

Google Analytics (2018). Aperçu des rapports "Type d'audience". Récupéré de https://support.google.com/analytics/answer/1012034?hl=fr

Granville, K. (2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. Récupéré de https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Greffet, F. et Wojcik, S. (2014). La citoyenneté numérique. *Réseaux*, (2), 125-159.

Greenwald, G. et MacAskill, E. (2013, 7 juin). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Récupéré de https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US surveillance state.* Macmillan.

Gouvernement du Canada (2018). Groupe des cinq. Récupéré de http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=&index=alt&srchtxt=FIVE%20EYES

Härmälä, T. (2014). *Étude de la résistance dans la pensée politique de Michel Foucault* [Mémoire de maîtrise]. Université de Jyväskylä. Récupéré de https://jyx.jyu.fi/bitstream/handle/123456789/43273/URN:NBN:fi:jyu-201404251575.pdf?sequence=1

Hauge, M. V., Stevenson, M. D., Rossmo, D. K. et Le Comber, S. C. (2016). Tagging Banksy: Using geographic profiling to investigate a modern art mystery. *Journal of Spatial Science*, *61*(1), 185-190.

Heyning, K. E. (1997). Rationality, Technology and Reform: Examining the" Governmentality"of Certification Change. Récupéré de https://files.eric.ed.gov/fulltext/ED407363.pdf

Hooper, D. et Whyld, K. (1987). *The Oxford companion to chess*. USA: Oxford University Press.

Howe, D. C. et Nissenbaum, H. (2017). Engineering Privacy and Protest: a Case Study of AdNauseam. Dans *CEUR Workshop Proceedings* (*1873*, 57-64).

Huff, R. (2018). Gouvernementalité. *Encyclopædia Universalis*. Récupéré de http://www.universalis-edu.com/encyclopedie/gouvernementalite/

IBM (s. d.). Le Big Data à l'écoute de votre business. Récupéré de https://www-01.ibm.com/software/fr/data/bigdata/

Ici Radio-Canada (2017). Il y a 10 ans, l'iPhone entrait dans nos vies. Récupéré de https://ici.radio-canada.ca/nouvelle/1042310/iphone-lancement-etats-unis-canada-archives

Ici Radio-Canada (2018). Comment fonctionne Tor, le navigateur du web invisible? Récupéré de https://ici.radio-canada.ca/premiere/emissions/la-sphere/segments/entrevue/69847/tor-web-invisible-dark-web-genevieve-lajeunesse

Ici Radio-Canada (2018). Google suit vos déplacements… que vous le vouliez ou non. Récupéré de https://ici.radio-canada.ca/nouvelle/1117814/google-donnees-localisation-parametres-confidentialite-android-iphone

International Working Group on Data Protection in Telecommunications (2014). *Working Paper on Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics*. Récupéré de http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf?1407931243

Janks, H. (1997). Critical discourse analysis as a research tool. *Discourse: studies in the cultural politics of education*, *18*(3), 329-342.

Koenig, G., Landreau, I., Peliks, G., Binctin, N., Pez-Pérard, V. et Léger, L. (dir.) (2018). *Mes data sont à moi*. Récupéré de https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: Sage.

Kitchin, R. et Dodge, M. (2011). *Code/space: Software and everyday life*. Cambridge : The MIT Press.

Lafleur, S. (2017). Penser la gouvernementalité après Foucault. Politique et *Sociétés*, *36*(3), 141-159.

Lamoureux, A. (2000). *Recherche et Méthodologie en Sciences humaines*. Québec : Études vivantes.

Larousse (s. d.) Far West. Récupéré de https://www.larousse.fr/dictionnaires/francais/far_west/32929

La Presse (2018). Facebook en fâcheuse posture. Récupéré de http://plus.lapresse.ca/screens/58cd7f3d-962d-485e-ad1d-47b1731b55a0__7C___0.html

La Quadrature du Net (2016). Si vous êtes le produit, ce n'est pas gratuit. Récupéré de https://www.laquadrature.net/fr/si-vous-etes-le-produit

Levine, Y. (2018). The Tor Files: Transparency for the Dark Web [Full FOIA Cache]. *Surveillance Valley*. Récupéré de https://surveillancevalley.com/the-tor-files/thetor-files-transparency-for-the-dark-web-full-foia-cache

Lever, R. et Charpentrat, J. (2017). Zuckerberg s'excuse sans remettre en cause le modèle Facebook. *La Presse*. Récupéré de http://www.lapresse.ca/techno/201706/23/01-5110393-google-ne-lira plus-les-courriels-sur-gmail.php

Lipovetsky, G. (1983). *L'ère du vide : essais sur l'individualisme contemporain.* Éditions Gallimard.

Lyotard, J. F. (1979). *Les problèmes du savoir dans les sociétés industrielles les plus développées*. Québec : Gouvernement du Québec, Conseil des universités.

Madrigal, A. C. (2012). I'm Being Followed: How Google-and 104 Other Companies-Are Tracking Me on the Web. *The Atlantic*. Récupéré de https://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/

Malette, S. (2006). *La "gouvernementalité" chez Michel foucault.* [Mémoire de maîtrise]. Université Laval.

Martin, É. (2007). Le journalisme et la désymbolisation du monde pour une critique dialectique de la crise contemporaine du journalisme.

Martínez, C. (2017). The struggles of everyday life: How children view and engage with advertising in mobile games. *Convergence - The International Journal of Research into New Media Technologies*, 1-20. doi: 10.1177/1354856517743665

Marx, K. (1867). *Le capital*. Récupéré de http://classiques.uqac.ca/classiques/Marx_karl/capital/capital.html

McDonald, A. M. et Cranor, L. F. (2008). The cost of reading privacy policies. *ISJLP*, *4*, 543.

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G. et Guo, S. (2016). Protection of big data privacy. *IEEE access*, *4*, 1821-1834.

Melody, W. H. (2006). Technologies de l'information et des communications. *L'encyclopédie canadienne.* Récupéré de https://www.thecanadianencyclopedia.ca/fr/article/communications-technologies-de-linformation-et-des-tic

Ménard, M. et Mondoux, A. (s. d.). Big Data, médiation symbolique et accélération sociale.

Ménard, M., Mondoux, A., Ouellet, M. et Bonenfant, M. (2016). Big Data, gouvernementalité et industrialisation des médiations symboliques et politico institutionnelles. *Interfaces numériques*, *5*(2), 1-26.

Ménard, M. et Mondoux, A. (2018). Big Data, médiation symbolique et accélération sociale. Dans *@ la recherche du temps* (217-236). ERES.

Metcalf, J. et Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society*, *3*(1), 1-14. doi: 10.1177/2053951716650211

Mondoux, A. (2007). *Technique, individuation et (re) production sociale : la musique numérique MP3*. [Doctoral dissertation, Université du Québec à Montréal].

Mondoux, A. (2011). Identité numérique et surveillance. *Les Cahiers du numérique*, *7*(1), 49-59.

Mongeau, P. (2008). Réaliser son mémoire ou sa thèse : Côté jeans et côté tenue de soirée. Québec : Presses de l'Université du Québec.

Mosenia, A., Dai, X., Mittal, P. et Jha, N. (2017). PinMe: Tracking a Smartphone User around the World. *IEEE Transactions on Multi-Scale Computing Systems*.

Office québécois de la langue française. [2006]. Pirate informatique. Dans *Dictionnaire de la comptabilité et de la gestion financière*. Récupéré de http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=502840

Office québécois de la langue française. [2002]. Pixel espion. Dans *Le grand dictionnaire terminologique*. Récupéré de http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367061

Office québécois de la langue française. [2013]. Réseau privé virtuel. Dans *Le grand dictionnaire terminologique.* Récupéré de https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/reseau_prive_virtuel.html

Office québécois de la langue française. [2017]. Web invisible. Dans *Le grand dictionnaire terminologique.* Récupéré de http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8370264

Ouellet, M. (2015). Cybercapitalisme et totalitarisme. *Relations*, *776*, 18-19.

Ouellet, M., Ménard, M., Bonenfant, M. et Mondoux, A. (2015). Big Data et quantification de soi : La gouvernementalité algorithmique dans le monde numériquement administré. *Canadian Journal of Communication*, *40*(4), 597.

OpenMedia (2013). More than 30 organizations unite to safeguard Canadians' privacy rights amid spy agency scandal. Récupéré de https://openmedia.org/en/press/more-30-organizations-unite-safeguard-canadians'-privacy-rights-amid-spy-agency-scandal

OpenMedia (2017). Internet Mapping: See Where Your Data Travels. Récupéré de https://openmedia.org/en/ixmaps-see-where-your-data-travels

Proulx, S. (2002, mars). Trajectoires d'usages des technologies de communication: les formes d'appropriation d'une culture numérique comme enjeu d'une «société du savoir». Dans *Annales des télécommunications*, *57*(3-4), 180-189. Springer-Verlag.

Proulx, S. et Choon, M. J. K. (2011). L'usage des réseaux socionumériques : une intériorisation douce et progressive du contrôle social. *Hermès, La Revue*, (1), 105-111.

Pew Research Center (2015) Americans' Privacy Strategies Post-Snowden. Washington, D. C. Récupéré de http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Pieuvre (2017). Les données « anonymes » de millions d'Allemands dévoilées au grand jour. Récupéré de http://www.pieuvre.ca/2017/08/01/les-donnees-anonymes-de-millions-dallemands-devoilees-au-grand-jour/

Quantin, P. (1987). *Les Origines de l'idéologie*. Paris : Economica.

Quivy, R. et Campenhoudt, V. L. (1988). *Manuel de recherche en sciences sociales.* Paris : Dunod.

Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). 2016/679. (2018). Récupéré de https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

Revel, J. (2002). *Le vocabulaire de Foucault.* Paris : Ellipse.

Rochon, F. (2014). Michel Foucault et le souci de vérité/Du gouvernement des vivants. Cours au Collège de France (1979-1980), de Michel Foucualt, EHESS, Gallimard et Seuil, 380 p./Cahier de l'Herne Michel Foucault. Sous la direction de Philippe Artières, Jean-François Bert et Judith Revel, Éditions de l'Herne, 415 p. *Spirale: arts• lettres• sciences humaines*, (247), 76-78.

Roesner, F., Kohno, T. et Wetherall, D. (2012, avril). Detecting and defending against third-party tracking on the web. Dans *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementatio*n (p. 1-28). San Jose : USENIX Association.

Rouvroy, A. (2015). Au moins dans un système totalitaire on sait à quoi on a affaire. *Rue89, 28.*

Rouvroy, A. et Berns, T. (2010). Le nouveau pouvoir statistique. *Multitudes*, (1), 88-103.

Rouvroy, A. et Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : Le disparate comme condition d'individuation par la relation? *Réseaux, 177*(1), 163-196. doi: 10.3917/res.177.0163.

Rouvroy, A., et Stiegler, B. (2015). Le régime de vérité numérique. De la gouvernementalité algorithmique à un nouvel État de droit. *Socio. La nouvelle revue des sciences sociales*, (4), 113-140.

Sanchez-Vasquez, A. et Nair, K. (1977). La philosophie de la praxis comme nouvelle pratique de la philosophie. *L'Homme et la société, 43*(1), 141-149.

Schneider, W. (2003). The Role and Status of DoD Red Teaming Activities. *Defense Science Board.*

Sibille, B. (2006). Gouvernance et gouvernementalité. *Chaire de recherche du Canada en citoyenneté et gouvernance*. Récupéré de http://www.cccg.umontreal.ca/pdf/sibille_gouvernance_et_gouvernementalite.pdf

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, *126*, 1880.

Statista (2018a). Facebook's annualized revenue per user from 2012 to 2017 (in U.S. dollars) [Tableau]. Récupéré de https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/

Statista (2018b). Number of daily active Facebook users worldwide as of 1st quarter 2018 (in millions) [Tableau]. Récupéré de https://www.statista.com/statistics/346167/facebook-global-dau/

Stiegler, B. (2005). Individuation et grammatisation : quand la technique fait sens... *Documentaliste-Sciences de l'Information*, *42*(6), 354-360.

Stiegler, B. (2015). *La société automatique : 1. L'avenir du travail*. Paris : Fayard.

Sushcheva, N. et Fontanel, J. (2018). Les GAFAM.

TAMS Analyzer (s. d.). [Logiciel]. Récupéré de http://tamsys.sourceforge.net

Tencer, D. (2017). Canadians' Internet Data Affected As Trump Cancels Privacy Rules. *The Huffington Post Canada*. Récupéré de http://www.huffingtonpost.ca/2017/01/31/internet-privacy-canada-trump-executive-order_n_14500862.html

The White House (2017). Executive Order: Enhancing Public Safety in the Interior of the United States. Récupéré de https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

Tor (2018). Le guide d'utilisation du navigateur Tor. Récupéré de https://tb manual.torproject.org/fr/about-tor-browser.html

Tzu, S. (~400 av. J.-C. / 2015). *L'art de la guerre*. Paris : Pluriel.

Vallée, K.-P. (2018). Intel, AMD, Arm : deux failles de sécurité majeures menacent votre ordinateur. *Ici Radio-Canada*. Récupéré de https://ici.radio-canada.ca/nouvelle/1076270/spectre-meltdown-intel-amd-arm-processeurs-piratage-securite-informatique

Van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & society*, *4*(2), 249-283.

Van Dijk, T. A. (1995). Aims of critical discourse analysis. *Japanese discourse*, *1*(1), 17-28.

Van Dijk, T. A. (2000). *Ideology and discourse: A multidisciplinary introduction.* Pompeu Fabra University, Barcelona.

Van Dijk, T. A. (2006). Ideology and discourse analysis. *Journal of political ideologies*, *11*(2), 115-140.

Van Dijk, T. A. (2008). *Discourse and context: A sociocognitive approach.* Cambridge: Cambridge University Press.

Wodak, R. et Meyer, M. (2009). Critical discourse analysis: history, agenda, theory and methodology. *Methods of critical discourse analysis*, 1-34.

Wolff, F. (2015). La politique divise, le politique rassemble. *Le Monde*. Récupéré de https://www.lemonde.fr/idees/article/2015/02/11/la-politique-divise-le-politique-rassemble_4574280_3232.html

Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and information technology*, *12*(4), 313-325. doi: 10.1007/s10676-010-9227-5

Zine, M. C. (2010). La pensée et l'action dans la perspective sociologique de Michel de Certeau. *Laval théologique et philosophique*, *66*(2), 407–423. doi: 10.7202/044848ar

Zuckerberg, M. (2018). "We have a responsibility to protect your data, and if we can't then we don't deserve it." Read Mark's thoughts on user data, Cambridge Analytica and Facebook's next steps. *Facebook*. Récupéré de https://www.facebook.com/facebook/posts/10157217558586729

Zuckerberg, M. (2019). A Privacy-Focusad Vision for Social Networking. *Facebook*. Récupéré de https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/