Université de Montréal

Surveillance électronique et métadonnées.
Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada?

par Alexandre Thibeault

Faculté de droit

Mémoire présenté à la Faculté des études supérieures en vue de
l'obtention du grade de Maîtrise en droit international (LL.M.)

Mars 2015

RÉSUMÉ ET MOTS CLÉS

Résumé : Ce mémoire traite de la portée de la protection constitutionnelle du droit à la vie privée informationnelle au Canada, au regard de la surveillance électronique gouvernementale à grande échelle des métadonnées des communications électroniques, à des fins de sécurité nationale. Il est soutenu, après une présentation de l'importance démocratique de la vie privée, de même que de la nature et de la portée de certaines activités gouvernementales de surveillance électronique, que le cadre d'analyse du « Biographical core », qui conditionne l'étendue de la protection de la vie privée informationnelle en droit constitutionnel canadien, est susceptible d'inclure les métadonnées des communications électroniques. Cette position est appuyée par un argumentaire juridique fondé sur les règles d'interprétation et la jurisprudence constitutionnelle pertinente. Cet argumentaire se trouve renforcé par potentiel considérablement révélateur des métadonnées, des particularités propres aux activités de surveillance électronique analysées, ainsi que des implications non-juridiques soulevées par ces dernières.

Mots clés : sécurité nationale, lutte au terrorisme, surveillance électronique, métadonnées, technologies de l'information, droit à la vie privée, droit constitutionnel, démocratie, Canada

SUMMARY AND KEY WORDS

Summary: This master's thesis focuses on the scope of the Canadian constitutional protection of the right to privacy, in view of the wide scale governmental electronic surveillance of electronic communications metadata, conducted for national security purposes. It is argued, following a detailed presentation of the nature and extent of certain specific governmental electronic surveillance activities, that the « Biographical core » analytical framework, governing the scope of the protection granted to informational privacy in Canadian constitutional law, is most likely applicable to electronic communications metadata. This position is directly supported by the relevant constitutional interpretation rules and cases. This is particularly true in light of the fact that metadata are, inherently, potentially significantly revealing, especially considering the capacities of an array of electronic surveillance activities, as well as the non-legal implications they entail for privacy.

Key words : national security, war on terror, electronic surveillance, metadata, information technologies, right to privacy, constitutional law, democracy, Canada

TABLE DES MATIÈRES

RÉSUMÉ ET MOTS CLÉS ..... **I**

SUMMARY AND KEY WORDS ..... **II**

TABLE DES MATIÈRES ..... **III**

LISTE DES ABBRÉVIATIONS ..... **VI**

REMERCIEMENTS ..... **VIII**

INTRODUCTION **1**

1. LA VIE PRIVÉE AU XXIE SIÈCLE **9**

Introduction 9

1.1. L'importance démocratique du droit à la vie privée 10

1.1.1. La vie privée comme vecteur de réalisation individuelle 14

1.1.2. La vie privée comme vecteur de cohésion sociale 17

1.2. La surveillance électronique gouvernementale et la collecte des métadonnées 22

1.2.1. Le concept de métadonnées et ses implications 23

1.2.1.1. Les métadonnées : une définition 24

1.2.1.2. La distinction contenu-métadonnée 27

1.2.1.3. Les métadonnées à l'ère du « Big Data » 28

1.2.1.4. Le potentiel très révélateur des métadonnées 30

1.2.2. La surveillance électronique 33

1.2.2.1. La surveillance : quelques précisions terminologiques 34

1.2.2.1.1. La surveillance 34

1.2.2.1.2. La surveillance électronique 35

1.2.2.2. L'accroissement de la surveillance post-11 septembre 2001 37

1.2.2.3. La surveillance électronique des métadonnées 40

1.2.2.4. Le cas du Canada 42

Conclusion provisoire 46

2. LA PROTECTION DU DROIT À LA VIE PRIVÉE AU CANADA **50**

Introduction 50

2.1. Le cadre normatif établi par le droit canadien 51

2.1.1. La protection constitutionnelle de la vie privée 52

2.1.1.1. L'article 7 de la Charte canadienne des droits et libertés 53
2.1.1.1.1. La protection de la liberté : l'aménagement d'une sphère d'autonomie individuelle 54
2.1.1.1.2. La protection de la sécurité : le respect de l'intégrité individuelle 57
2.1.1.2. L'article 8 de la Charte canadienne des droits et libertés 58
2.1.1.2.1. L'attente raisonnable en matière de vie privée 61
2.1.1.2.1.1. Le critère de l'« attente raisonnable » 62
2.1.1.2.1.2. Les intérêts protégés par la vie privée 66
2.1.1.2.2. Le caractère raisonnable d'une fouille, perquisition ou saisie : la violation de la protection conférée par l'article 8 70
2.1.1.2.2.1. La détermination du caractère raisonnable d'une fouille, perquisition ou saisie 71
2.1.1.2.2.2. La recevabilité des éléments de preuve 72
2.1.2. Les régimes législatifs de protection de la vie privée 74
2.2. La vie privée informationnelle : le cadre d'analyse du « Biographical core » 77
2.2.1. La vie privée informationnelle comme modalité d'aménagement de l'identité individuelle 78
2.2.2. La protection normative de la vie privée informationnelle 80
2.2.3. La détermination de l'objet d'une fouille, perquisition ou saisie en matière de vie privée informationnelle 85
Conclusion provisoire 91
3. VERS UNE NOUVELLE CONCEPTION DE LA VIE PRIVÉE? 95
Introduction 95
3.1. La protection juridique des métadonnées des communications électroniques 97
3.1.1. Les métadonnées des communications électroniques comme renseignements biographiques d'ordre personnel 98
3.1.1.1. L'agrégation et l'analyse des métadonnées, ou le caractère fondamentalement invasif de la surveillance gouvernementale 99
3.1.1.2. La désuétude de la distinction contenu-métadonnée dans le contexte contemporain 102
3.1.1.3. La qualité intrinsèque des renseignements visés par la surveillance électronique gouvernementale 103
3.1.2. L'interprétation de l'article 8 au regard de l'environnement technologique contemporain 105
3.1.2.1. L'interprétation téléologique de l'article 8 de la *Charte canadienne* 106
3.1.2.2. L'article 8 face aux nouvelles technologies de l'information et des communications : la reconnaissance d'une sphère privée 112

3.1.2.2.1. La prise en considération de l'évolution du contexte technologique 112

3.1.2.2.2. Les nouvelles technologies de l'information et des communications et les métadonnées des communications électroniques 114

3.2. La surveillance des métadonnées des communications électroniques au sein du contexte global 124

3.2.1. Les implications sociales de la surveillance électronique des métadonnées 125

3.2.1.1. L'équilibre entre le maintien de la sécurité nationale et la protection des droits fondamentaux 125

3.2.1.2. Le caractère profondément invasif de l'infrastructure de surveillance contemporaine 128

3.2.1.3. Le potentiel d'abus 130

3.2.1.4. Les risques pour la vie privée 133

3.2.2. La surveillance électronique des métadonnées dans le contexte mondial 135

3.2.2.1. L'approche empruntée par les États-Unis d'Amérique 136

3.2.2.2. Le positionnement des organisations non gouvernementales 137

3.2.2.3. L'innovation technologique entrepreneuriale au service de la vie privée 139

Conclusion provisoire 143

CONCLUSION 148

BIBLIOGRAPHIE 157

LISTE DES ABBRÉVIATIONS

Abréviations relatives à la législation

Canada

art.	article
c.	chapitre
C.C.S.M.	Continuing Consolidation of the Statutes of Manitoba
L.C.	Lois du Canada
L.Q.	Lois du Québec
L.R.C.	Lois révisées du Canada
L.R.Q.	Lois refondues du Québec
R.S.A.	Revised Statutes of Alberta
R.S.B.C.	Revised Statutes of British Columbia
R.S.M.	Revised Statutes of Manitoba
R.S.N.L.	Revised Statutes of Newfoundland and Labrador
R.S.O.	Revised Statutes of Ontario
R.S.P.E.I.	Revised Statutes of Prince Edward Island
R.S.S.	Revised Statutes of Saskatchewan
R.S.Y.	Revised Statutes of Yukon
R.-U.	Royaume-Uni
S.B.C.	Statutes of British Columbia
S.N.B.	Statutes of New Brunswick
S.N.L.	Statutes of Newfoundland and Labrador
S.N.S.	Statutes of Nova Scotia
S.N.W.T.	Statutes of the Northwest Territories
S.N.W.T. (Nu.)	Statutes of the Northwest Territories (Nunavut)
S.A.	Statutes of Alberta
S.O.	Statutes of Ontario
S.S.	Statutes of Saskatchewan

États-Unis

Pub. L. No.	Public Law Number
U.S.C.	United States Code
U.S. Const.	United States Constitution

Abréviations relatives à la jurisprudence

Canada

CSC	Canada Supreme Court Cases
ONCA	Ontario Court of Appeal
R.C.S.	Recueil des arrêts de la Cour suprême du Canada
SKCA	Saskatchewan Court of Appeal

États-Unis

U.S.	United States Supreme Court Reports

Abréviations relatives à la doctrine

Alta. L. Rev.	Alberta Law Review
Cal. L. Rev.	California Law Review
Can. Crim. L. Rev.	Canadian Criminal Law Review
Can. J. L. & Tech.	Canadian Journal of Law and Technology
C. de D.	Les Cahiers de droit
C.L.Q.	The Criminal Law Quarterly
Harv L. Rev.	Harvard Law Review
Ohio N. U. L. Rev.	Ohio Northern University Law Review
Phil. & Pub. Aff.	Philosophy & Public Affairs
R.D. McGill	Revue de droit de McGill
R.D.T.U.O.	Revue de droit & technologie de l'Université d'Ottawa
R.J.T.	Revue juridique Thémis
Sask L. Rev.	Saskatchewan Law Review
S.C.L.R.	Supreme Court Law Review
S.F.P.B.Q.	Service de la formation permanente du Barreau du Québec
S.L.R.	Stanford Law Review
U.B.C. L. Rev.	University of British Columbia Law Review
U.T. Fac. L. Rev.	University of Toronto Faculty of Law Review
U.T.L.J.	University of Toronto Law Journal
Yale L.J.	Yale Law Journal

REMERCIEMENTS

Je tiens, d'entrée de jeu, à exprimer mes plus sincères remerciements au Professeur Karim Benyekhlef. Je me permets de souligner l'apport considérable de ses judicieux conseils, sa grande patience et son implacable rigueur, sans lesquels ce projet intellectuel n'aurait su voir le jour dans sa forme actuelle.

Je désire ensuite remercier certains collègues et amis pour leur contribution à ma démarche intellectuelle. Je pense ici, entre autres, à Me Jean-Sébastien Sauvé, que je remercie pour sa relecture critique de la deuxième partie de ce mémoire, ainsi que pour ses commentaires toujours pertinents. Je pense également ici à Pierre-Luc Déziel, dû à nos nombreuses – et très éclairantes – discussions sur les considérations théoriques et conceptuelles entourant le droit à la vie privée, ainsi qu'à Me Gabriel Faure, pour ses sages conseils portant notamment sur le processus de recherche aux cycles supérieurs.

Il me faut bien entendu ici saluer le soutien indéfectible de mes proches, à commencer par ma conjointe, Valérie, mes parents, Jocelyne et Claude, et mes frères, Vincent et Samuel.

Finalement, je fais part de toute ma gratitude à la Faculté de droit de l'Université de Montréal, en raison de son généreux appui financier. Cet appui fut rendu possible par la grande générosité du cabinet Heenan Blaikie, du Fonds J.A. Louis-Lagassé, ainsi que de la Faculté des études supérieures et postdoctorales.

INTRODUCTION

> *The efforts to limit official surveillance over man's thoughts, speech, private acts, confidential communications, and group participation has for centuries been a central part of the struggle for liberty in Western society. This search for personal and group privacy has been waged against kings and legislatures; churches, guilds, manor lords, and corporations; sheriffs, welfare investigators, and political police.*
>
> Alan F. Westin[1]

Les enjeux inhérents à la sécurité nationale et à la lutte au terrorisme occupent, depuis septembre 2001, une place prépondérante dans l'élaboration des politiques publiques occidentales. Les attentats de nature terroriste commis dernièrement au Canada[2], en Australie[3] et en France[4] contribuent à exacerber cette tendance. Dans la foulée de ces attentats, le gouvernement du Canada a déposé, le 30 janvier 2015, le projet de loi C-51 à la Chambre des communes, lequel vise notamment à accroître les pouvoirs du Service canadien du renseignement de sécurité et à criminaliser la promotion du terrorisme[5]. Le gouvernement français a, pour sa part, récemment annoncé la création de 2 680 postes visant spécifiquement à lutter contre le terrorisme[6]. Les autorités britanniques songent, quant à elles, à déposer

---

[1] Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967, p. 67.

[2] Josh WINGROVE, Steven CHASE, Bill CURRY et Jill MAHONEY, « Attack on Ottawa : PM Harper cites terrorist motive », *The Globe and Mail* (22 octobre 2014), en ligne : <http://www.theglobeandmail.com/news/politics/parliament-shooting/article21217602/> (dernière consultation le 18 février 2015).

[3] BBC NEWS, « Sydney siege: Hostages held in Lindt cafe », *BBC News* (15 décembre 2014), en ligne : <http://www.bbc.com/news/world-australia-30473983> (dernière consultation le 18 février 2015).

[4] BBC NEWS, « Charlie Hebdo attack: Three days of terror », *BBC News* (14 janvier 2015), en ligne : <http://www.bbc.com/news/world-europe-30708237> (dernière consultation le 18 février 2015).

[5] Laura PAYTON, « Anti-terrorism powers: What's in the legislation? », *CBC News* (30 janvier 2015), en ligne : <http://www.cbc.ca/news/politics/anti-terrorism-powers-what-s-in-the-legislation-1.2937964> (dernière consultation le 18 février 2015).

[6] David REVAULT D'ALLONNES et Bastien BONNEFOUS, « Manuel Valls annonce la création de 2 680 postes pour lutter contre le terrorisme », *Le Monde* (21 janvier 2015), en ligne : <http://www.lemonde.fr/politique/article/2015/01/21/manuel-valls-annonce-la-creation-de-2680-emplois-pour-lutter-contre-le-terrorisme_4560334_823448.html> (dernière consultation le 18 février 2015).

prochainement un projet de loi ayant pour objet de priver les présumés terroristes de tout « refuge » en ligne[7]. Un tel empressement serait susceptible de nous laisser croire que ces préoccupations sécuritaires sont propres à l'air du temps, voire spécifiquement caractéristiques de notre époque. Or, il n'en est rien.

Selon Karim Benyekhlef, « l'histoire et la philosophie font […] de la sécurité l'une des premières missions de l'État »[8]. L'initiative de l'exercice des fonctions sécuritaires ne saurait toutefois être attribuée à l'État moderne. Avant même l'avènement de cette forme relativement récente d'organisation politique, le souverain, quel qu'il soit, s'est historiquement arrogé la mission sécuritaire, notamment afin d'asseoir son pouvoir[9]. Ainsi, l'apparition des premières formes de regroupements sociaux structurés a provoqué l'émergence d'organisations ayant comme unique objectif d'assurer la sécurité du groupe contre ses ennemis et toute autre forme de menace, qu'elle trouve sa source au sein même du groupe ou lui soit externe[10]. Pour ce faire, l'Homme a, depuis la nuit des temps, systématiquement tenté d'acquérir de

---

[7] Nicholas WATT, Rowena MASON et Ian TRAYNOR, « David Cameron pledges anti-terror law for internet after Paris attacks », *The Guardian* (12 janvier 2015), en ligne : <http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg> (dernière consultation le 18 février 2015).

[8] Karim Benyekhlef ajoute que, de tout temps, « la sécurité [a constitué] une *industrie* pour l'État qui y a eu recours régulièrement afin d'affermir sa souveraineté et y trouver un brillant prétexte pour établir une surveillance et un contrôle toujours croissant sur ses citoyens, leurs activités et leurs affaires ». Voir Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation*, Montréal, Thémis, 2008, p. 685.

[9] *Id.*

[10] Par exemple, dans les États démocratiques contemporains, la sécurisation du groupe contre toute menace interne est généralement confiée aux organisations ayant un caractère policier, alors que la protection contre tout ennemi externe relève des organisations à caractère militaire.

l'information sur les intentions, les plans et les capacités de ses ennemis[11], qu'ils soient réels ou simplement perçus.

Le philosophe et historien grec Xénophon rapporte, par exemple, qu'il était dit de Cyrus le Grand, fondateur de l'Empire perse au 6e siècle av. J.-C., qu'il possédait « de nombreux yeux et oreilles »[12]. Loin d'être doté de pouvoirs surhumains, Cyrus avait mis en place un réseau de surveillance d'une proportion quasi moderne, articulé autour d'un système très élaboré de messagers chargés de recueillir et relayer une myriade d'informations sur l'empire, ses sujets et les opposants potentiels à l'empereur[13]. L'ampleur et l'efficacité du système étaient telles que Xénophon écrivit :

> In general people shied away from saying anything detrimental about the King, lest he be eavesdropping himself, or to do something that could damage him. It appeared he was ubiquitous. Thus not only dit no one dare tell anyone anything derogatory about Cyrus, everyone behaved at all times as if everyone within hearing were the eyes and ears of the King[14].

Bien qu'il ne s'agisse que d'un exemple parmi tant d'autres, il nous faut reconnaître que les activités de surveillance à des fins de sécurité – historiquement assimilées au concept d'espionnage – ont toujours occupé une place absolument centrale[15] au sein de toute forme d'organisation structurée du pouvoir, qu'il soit militaire, politique ou social[16].

---

[11] Sur ce sujet, Janusz Piekalkiewicz écrit que « [f]rom earliest times, people have tried to gain knowledge of the intentions, plans, and capabilities of their enemies. For this reason, what is called espionage has been in existence for thousands of years. This kind of work, often described as the second oldest profession, is presumably even older than the one jokingly called the oldest which, incidentally, frequently is employed in espionage ». Voir Janusz PIEKALKIEWICZ, *World History of Espionage : Agents, Systems, Operations*, Munich, Südwest Verlag, 1988, p. 29.

[12] *Id.*, p. 63.

[13] *Id.*

[14] *Id.*, p. 64.

[15] Nous n'aurions, par exemple, qu'à penser au rôle des éclaireurs carthagénois d'Hannibal, durant les Guerres puniques, à l'espionnage économique au sein de l'Empire byzantin, aux manœuvres de la diplomatie secrète

Plus spécifiquement, l'efficacité de telles activités a, de tout temps, reposé sur la disponibilité et la mise en place de méthodes, techniques et technologies adaptées au contexte environnant et permettant d'obtenir, de manière fiable et ciblée, les renseignements désirés. Or, il n'est un secret pour personne que nous vivons aujourd'hui dans un monde hautement connecté, dont les modes de communication s'accélèrent au rythme de leur multiplication, générant de ce fait des masses perpétuellement croissantes d'informations de toutes sortes[17]. Consciemment ou non, la très grande majorité des individus participent à ce phénomène, ne serait-ce qu'en raison de la prégnance des nouvelles technologies de l'information et des communications dans notre environnement contemporain et de leur utilisation quotidienne systématique. Le choc provoqué, en juin 2013, par les révélations d'Edward Snowden, selon lequel certaines politiques publiques de sécurité nationale impliqueraient, au sein même des démocraties occidentales, une surveillance électronique à grande échelle des citoyens, à commencer par les métadonnées de leurs communications électroniques[18], n'en fut donc

---

du cardinal Armand Jean du Plessis de Richelieu ou encore à l'affaire Dreyfus, jusqu'aux manoeuvres, montages, et subterfuges les plus récents des services de renseignement de par le monde. Pour plus de détails, voir J. PIEKALKIEWICZ, préc., note 11.

[16] Cette importance fut dramatiquement accrue – puis confortée – du fait de l'avènement de l'État bureaucratique wébérien, qui permit leur rationalisation, leur organisation et leur perfectionnement à l'échelle de l'ensemble de la population. C'est d'ailleurs à la même époque que ces activités prirent une forme relativement moderne, de manière à correspondre à ce que nous entendons aujourd'hui par « surveillance ». Pour plus d'information, voir Christopher DANDEKER, *Surveillance, Power and Modernity. Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge, Polity Press, 1990, p. 41-43. Il est néanmoins possible de retracer des exemples de collecte généralisée d'information à des fins sociales ou politiques aussi loin qu'à l'époque de la République romaine, sous la forme de registres d'aptitude au service militaire, ou encore au Moyen-âge, dans le cas du Domesday Book britannique de 1086, qui contenait plus de 13 000 dossiers individuels. Voir, à ce sujet, Toni WELLER, « The information state. An historical perspective on surveillance », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 57, à la page 57.

[17] Sur ce sujet, voir Viktor MAYER-SCHÖNBERGER et Kenneth CUKIER, *Big Data. A Revolution That Will Transform How We Live, Work and Think*, Londres, John Murray, 2013.

[18] Le concept de métadonnée réfère aux données permettant l'identification d'autres données. Des précisions contextuelles et techniques détaillées seront fournies au lecteur dans la première partie ce mémoire (1.2.1).

qu'accentué[19]. Dans ce contexte, il est aisé de concevoir le rôle central et l'importance qu'occupent les nouvelles technologies de l'information en matière de collecte de renseignements à des fins de sécurité. Bien que les activités gouvernementales visant à préserver la sécurité du territoire et des individus – dont participent la surveillance et la collecte de renseignements – constituent, nous le rappelons, « l'une des premières missions de l'État »[20], il nous faut reconnaître qu'elles risquent de porter atteinte à certains droits et libertés fondamentaux. Aussi indispensables soient-elles, il est donc essentiel que ces activités fassent l'objet, dans une mesure raisonnable, d'un encadrement juridique crédible et efficace. Les révélations d'Edward Snowden nous permettent néanmoins de douter, voire de croire, que certaines activités de surveillance gouvernementale, particulièrement en matière électronique, supposent la collecte de renseignements protégés, *à priori*, par le droit à la vie privée dont jouit, en démocratie, tout individu[21].

Historiquement conçu, en common law, comme un attribut du droit de propriété, le concept de vie privée fut, dès 1890, défini dans une perspective juridique, comme étant un « droit d'être laissé seul »[22]. La vie privée fut par la suite envisagée, par William L. Prosser,

---

[19] Pour une vue d'ensemble de ces révélations, leur pertinence et leur impact, voir Kenan DAVIS, Nadja POPOVICH, Kenton POWELL et Ewen MACASKILL, « NSA Files : Decoded », *The Guardian* (1 novembre 2013), en ligne : <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> (dernière consultation le 18 février 2015).

[20] K. BENYEKHLEF, préc., note 8, p. 685.

[21] L'acte de surveiller se trouverait renforcé, écrit Alan Westin, par la propension quasi-naturelle que semblent avoir les individus à l'envahissement de l'intimité d'autrui : « [a]t the individual level, this is based upon the propensity for curiosity that lies in each individual, from the time that as a child he seeks to explore his environment to his later conduct as an adult in wanting to know more than he learns casually about what is ''really'' happening to others ». Voir Alan WESTIN, « The origins of modern claims to privacy », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 56, à la page 67.

[22] Samuel D. WARREN et Louis D. BRANDEIS, « The Right to Privacy », (1890) 4-5 *Harv. L. Rev.* 193, 205. Nous reviendrons brièvement sur cet aspect dans la première partie du mémoire.

comme étant une sphère protégeant un faisceau d'intérêts individuels variés[23], avant d'être conceptualisée par Alan F. Westin, à titre de composante essentielle de la liberté individuelle, définie en quatre objets, à savoir la solitude, l'intimité, l'anonymat et la réserve[24]. Toutefois, quoiqu'en disent les auteurs sur le plan conceptuel, la vie privée, dans toutes ses dimensions, est aujourd'hui susceptible de se trouver gravement affectée par la teneur de certaines activités de surveillance gouvernementale.

À la lumière de ces circonstances, nous avons décidé de nous interroger sur l'étendue de la protection constitutionnelle de la vie privée informationnelle en droit canadien, au regard de la surveillance à grande échelle des métadonnées à des fins de sécurité nationale. Plus spécifiquement, nous réfléchirons à la question suivante :

> Le cadre d'analyse du « Biographical core », qui conditionne la portée de la protection accordée à la vie privée informationnelle en vertu de l'article 8 de la *Charte canadienne des droits et libertés*[25], est-il susceptible d'inclure les métadonnées des communications électroniques?

Le choix de cette question de recherche nous incite à reconnaître, d'emblée, l'impact considérable des nouvelles technologies de l'information et des communications sur notre compréhension des fondements juridiques du droit à la vie privée[26]. Ainsi, nous estimons que le droit constitutionnel canadien constitue l'outil le mieux adapté nous permettant

---

[23] William L. PROSSER, « Privacy », (1960) 48-3 *Cal. L. Rev.* 383, 389.

[24] A. F. WESTIN, préc., note 1, p. 7, 31-32 et s.

[25] *Charte canadienne des droits et libertés*, Partie 1 de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.) [*Charte canadienne*].

[26] Karim Benyekhlef écrit, à ce sujet : « [e]n tout état de cause, les technologies de l'information et de la communication ne manquent pas de remettre en cause plusieurs présupposés du droit à la vie privée. […] Fondé sur le concept de territorialité (le domicile, le bureau, les espaces publics en contrechamp) et un certain statisme de l'information, le droit à la vie privée est bousculé dans ses fondements même par l'ubiquité de l'information, sa circulation incessante, sa très facile reproductibilité et sa déterritorialisation ». Voir Karim BENYEKHLEF et Esther MITJANS (dir.), *Circulation internationale de l'information et sécurité*, Montréal, Thémis, 2012, p. XI.

d'entreprendre la réflexion au cœur de ce mémoire, dans la mesure où son recours présuppose la prise en compte de la réalité politique et sociale contemporaine, dans son acception la plus large. Une telle approche nous semble, ultimement, nécessaire à l'appréhension de l'importance des nouvelles technologies de l'information et des communications au sein de l'ordre normatif canadien. Notre analyse constitutionnelle canadienne sera toutefois, concrètement, bonifiée par l'intégration, lorsque pertinente, de sources et d'éléments internationaux[27]. Qui plus est, la pertinence de notre démarche de recherche repose en grande partie, tel que nous le verrons, sur l'importance du droit à la vie privée et le caractère approprié de sa protection constitutionnelle, ainsi que sur la potentielle gravité des conséquences, à long terme, d'un contrôle inadéquat des activités de surveillance électronique gouvernementale.

Ceci étant, la première partie de ce mémoire sera consacrée à la présentation des éléments contextuels essentiels à l'approfondissement subséquent de notre réflexion, à savoir l'importance de la vie privée pour l'individu et la société, de même que la nature et la portée des activités de surveillance gouvernementale à grande échelle visant les métadonnées des communications électroniques. La deuxième partie portera sur l'établissement du cadre normatif canadien entourant la protection du droit à la vie privée, dans sa dimension constitutionnelle, ainsi que sur le traitement spécifique des particularités juridiques du cadre d'analyse du « Biographical core ». Finalement, la troisième et dernière partie sera consacrée

---

[27] Nous souscrivons, à cet égard, à la position de Karim Benyekhlef, lorsqu'il soutient que « [l]e droit constitutionnel ne se satisfait […] plus à lui-même; il n'est plus autosuffisant en quelque sorte puisque ses destinataires s'inspirent, crescendo, des décisions et opinions des juridictions étrangères, régionales et internationales et des travaux des institutions non juridictionnelles dans son interprétation et son application ». Voir K. BENYEKHLEF, préc., note 8, p. 661-662.

au cœur de notre réflexion, donc à la capacité du cadre d'analyse du « Biographical core » à protéger adéquatement les métadonnées des communications électroniques, au regard de leur surveillance à grande échelle à des fins de sécurité.

Bref, précisons, avant de plonger dans le vif du sujet, que toute étude sérieuse de la question de la surveillance gouvernementale à des fins de sécurité requiert la prise en considération d'une panoplie d'éléments et de facteurs fondamentalement complexes – et parfois diamétralement opposés – et qu'en conséquence, on ne saurait déceler, dans la réflexion présentée dans ce mémoire, de prise de position morale particulière. Le Procureur général de l'Australie affirmait, par ailleurs, récemment :

> Some, usually those with a better informed appreciation of the capabilities and danger of sophisticated modern terrorism, would wish for fewer limitations on intelligence gathering in the name of public safety. Others, most commonly those who do not bear responsibility for the protection of the public and who have the luxury of approaching the question from a largely philosophical or legalistic perspective, argue that there should be much wider limitations upon the collection of intelligence[28].

La fragilité inhérente à tout dilemme moral en cette matière nous incite donc à aborder cette aventure intellectuelle avec le recul qui s'impose. La recherche présentée dans ce mémoire est à jour au 1er janvier 2015.

---

[28] George BRANDIS, « The more intelligence I read, the more conservative I become », *The Guardian* (18 avril 2014), en ligne : <http://www.theguardian.com/commentisfree/2014/apr/09/the-more-intelligence-i-read-the-more-conservative-i-become> (dernière consultation le 18 février 2015).

1. LA VIE PRIVÉE AU XXI[E] SIÈCLE

> *It is helpful to start by seeking to identify those features of human life that would be impossible – or highly unlikely – without some privacy. Total lack of privacy is full and immediate access, full and immediate knowledge, and constant observation of an individual. In such a state, there would be no private thoughts, no private places, no private parts. Everything an individual did and thought would immediately become known to others. There is something comforting and efficient about total absence of privacy for all.* […] *Criminality would cease, for detection would be certain, frustration probable, and punishment sure. The world would be safer, and as a result, the time and resources now spent on trying to protect ourselves against human dangers and misrepresentations could be directed to other things. This comfort is fundamentally misleading, however. Some human activities only make sense if there is some privacy.* […] *We do not choose against total lack of privacy only because we cannot attain it, but because its price seems much too high.*
>
> Ruth Gavison[29]

Introduction

Il nous apparaît approprié d'entreprendre cette réflexion sur notre conception de la vie privée et la surveillance électronique des métadonnées par l'établissement des fondements et des assises conceptuelles, juridiques et factuelles essentielles à l'analyse de notre question de recherche. Cette partie aura comme objectif de permettre au lecteur de pleinement saisir l'importance et la valeur de la vie privée pour les individus comme pour la société et ce, particulièrement au regard de la teneur des activités de surveillance électronique gouvernementale des métadonnées. Bien que générale, cette partie s'avère intellectuellement nécessaire au développement ultérieur et à la présentation logique de notre réflexion. Ainsi, nous nous intéresserons tout d'abord brièvement, dans une première sous-partie, à l'importance du droit à la vie privée dans une perspective démocratique (1.1), afin de

---

[29] Ruth GAVISON, « Privacy and the Limits of Law », (1980) 89-3 *Yale L. J.* 421, 443.

contextualiser notre démarche de manière appropriée et d'illustrer l'importance des éléments qu'elle soulève. Pour ce faire, nous devrons sortir du cadre strictement juridique et recourir aux enseignements des sciences sociales, particulièrement de la philosophie. Ce n'est qu'une fois ce contexte établi qu'il nous sera possible, dans une seconde sous-partie, de nous intéresser au concept de métadonnée, puis d'aborder la question de leur surveillance électronique à grande échelle et à leur collecte par les autorités gouvernementales (1.2). Ultimement, cette première partie démontrera que la valeur fondamentale de la vie privée pour les individus comme pour la société, le caractère fondamentalement privé des informations que révèlent les métadonnées, de même que les risques que présentent toute activité de surveillance à grande échelle pour la démocratie, sont suffisamment importants pour justifier d'entreprendre, dans les parties subséquentes de ce mémoire, une réflexion quant à la protection juridique des métadonnées.

1.1. L'importance démocratique du droit à la vie privée

Il est fondamental, afin d'adéquatement cerner la portée de notre démarche de recherche, d'aborder d'entrée de jeu la question de l'importance de la vie privée[30]. Ce traitement permettra au lecteur, dans les parties subséquentes de ce mémoire[31], d'appréhender avec justesse les impacts considérables qu'est susceptible d'avoir la surveillance électronique totale des métadonnées sur la vie privée et d'en concevoir pleinement les nombreuses implications, lesquelles dépassent – et de loin – le cadre strictement juridique. Il nous permettra également

[30] Dans une perspective aussi bien individuelle et psychologique que sociale et culturelle.
[31] Nous référons ici à la sous-partie 1.2, dans laquelle il sera question des pratiques canadiennes de surveillance des métadonnées, à la partie II, où nous réfléchirons sur la conception juridique actuelle de la vie privée en droit canadien, ainsi qu'à la partie III, où nous approfondirons notre réflexion sur cette conception juridique.

de souligner la pertinence intellectuelle de notre recherche et l'importance d'entamer une réflexion visant à proposer un cadre d'analyse renouvelé du droit à la vie privée.

Cela étant, le concept de vie privée est, par définition, au cœur de la dichotomie ayant traditionnellement caractérisé, sur le plan historique, les domaines « privé » et « public ». Il est avancé que l'évocation dans la pensée occidentale de la relation entre le « moi », donc l'individu, voire l'espace privé, et la sphère externe, celle-là publique, remonte à l'an 429 avant notre ère, lorsque fut présentée pour la première fois la tragédie grecque *Œdipe roi*, du poète Sophocle[32]. Malgré l'incontestable intérêt culturel et littéraire de l'œuvre de Sophocle, il nous faut toutefois reconnaître que le concept de « vie privée » puise ses origines historiques dans les discussions philosophiques de l'Antiquité. Nous n'avons ici qu'à référer aux travaux d'Aristote[33] sur la distinction entre l'*Oikos*[34] et la *Polis*[35], qui ont posé les assises intellectuelles sur lesquelles repose encore aujourd'hui – ne serait-ce que partiellement – notre conceptualisation de la vie privée. Cette « division capitale » qui prévalait dans l'Antiquité entre les domaines public et privé structurait profondément, selon Hannah Arendt, toute la pensée politique des « Anciens »[36]. Toujours selon Arentd, « le domaine public était [alors] réservé à l'individualité; c'était le seul qui permettait à l'homme de montrer ce qu'il était

---

[32] Tracy B. STRONG, « self and politics », dans *Encyclopedia of Democratic Thought*, 641, Londres, Routledge, p. 641-642. Cette tragédie soulève le problème de la relation entre la question « qui suis-je? » et la réalisation du bien commun.

[33] Judith DECEW, « Privacy », dans The Stanford Encyclopedia of Philosophy, Fall 2013 Edition, Stanford, Center for the Study of Language and Information, en ligne : <http://plato.stanford.edu/entries/privacy/> (dernière consultation le 18 février 2015).

[34] Du grec ancien, signifiant « maison » et référant à la sphère personnelle d'un individu.

[35] Du grec ancien, signifiant « cité » et référant à l'espace public et collectif, par opposition à l'*Oikos*.

[36] Hannah ARENDT, *Condition de l'homme moderne*, coll. Agora, n°24, Paris, Calmann-Lévy, 1988, p. 66.

réellement, ce qu'il avait d'irremplaçable »[37]. Nous sommes toutefois, à la lumière des développements intellectuels et politiques majeurs survenus au cours des deux derniers millénaires, forcés de constater que cette affirmation ne représente plus adéquatement notre conception de la relation entre les domaines public et privé[38]. L'individualité étant aujourd'hui plutôt – du moins, principalement – associée à la sphère privée, c'est dans celle-ci que l'individu tend à vivre comme il est, sans artifice. Les fonctions échouant à l'espace public ont également profondément évolué. Nous reviendrons sur ces questions sous peu.

Plus récemment – et dans une perspective plus juridique – les auteurs américains Samuel D. Warren et Louis D. Brandeis écrivaient, en 1890, dans leur désormais célèbre article « The Right to Privacy » :

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[39] (Nos soulignements)

Il est vrai que les développements historiques survenus depuis la rédaction de ce passage rendraient possible une évaluation rétrospective de la gravité des risques invoqués par Warren

---

[37] *Id.*, p. 80. Plus loin, Arendt ajoute que « [l]e privé était comme l'autre face, sombre et cachée, du domaine public et si en étant politique on atteignait à la plus haute possibilité de l'existence humaine, en ne possédant point de place à soi (tel l'esclave) on cessait d'être humain » (p. 105). La professeure Julie E. Cohen rapporte quant à elle que le philosophe grec Socrate aurait affirmé que « [t]he unexamined life is not...worth living ». À ce sujet, voir Julie E. COHEN, « Examined Lives: Informational Privacy and the Subject as Object », 52-5 *S.L.R.* 1373, 1374.

[38] Bien qu'il ne soit pas ici de notre propos d'étudier en profondeur cet aspect, le changement de paradigme en question sera rapidement démontré de par la présentation du cadre juridique applicable au droit à la vie privée, dans la seconde partie de ce mémoire.

[39] S. D. WARREN et L. D. BRANDEIS, préc., note 22, 196.

et Brandeis[40]. Toutefois, la question du rapport entre les domaines public et privé, et plus particulièrement dans sa dimension concernant l'importance de la vie privée, pour l'individu comme pour la société, demeure aujourd'hui fondamentale à toute réflexion juridique sérieuse sur ce concept[41].

Le caractère essentiel de la vie privée auquel référaient Warren et Brandeis il y a désormais près de cent vingt-cinq ans, lorsqu'ils ont consacré le « droit d'être laissé seul », fut depuis analysé et étudié par de nombreux auteurs. Le regretté professeur Alan F. Westin avançait, en 1967, dans son ouvrage classique « Privacy and Freedom », que le désir d'un espace privé est si fondamental qu'il n'est pas limité à l'être humain et qu'il est possible de l'observer dans les processus biologiques et sociaux de toute forme de vie[42]. Bien que cette recherche d'un espace privé ne soit pas, à proprement parler, unique à l'humain, elle lui est essentielle sous plusieurs aspects, notamment parce qu'elle lui permet de se réaliser

---

[40] Arthur SCHAFER, « Privacy: A Philosophical Overview », dans Dale GIBSON (dir.), *Aspects of Privacy Law*, Toronto, Butterworths, 1980, p. 1 aux pages 2-3. Schafer considère que ces dangers peuvent être tempérés à la lumière d'un certain nombre de facteurs apparus durant le XXI^{e} siècle et ayant été bénéfiques à la vie privée des individus, tels que la migration urbaine et l'anonymat qui en découle, l'avènement de la famille nucléaire, l'affaiblissement des liens communautaires et des normes morales et l'accroissement de l'importance accordée aux aspirations et accomplissements individuels. Inversement, il considère qu'un nombre de tendances plus graves ont contribué à l'affaiblissement de la vie privée individuelle, à savoir notamment l'augmentation de la densité de population en milieu urbain, le recours massif au crédit, la commercialisation et le sensationnalisme des médias de masse, ainsi que les innovations technologiques découlant de l'informatisation.

[41] Il serait possible de consacrer un ouvrage entier uniquement à cette question. Or, puisque l'étude du caractère fondamental de la vie privée s'insère dans le cadre de la mise en contexte de notre démarche intellectuelle, nous ferons preuve ci-après d'un important exercice de concision, lequel, par la force des choses, ne nourrit aucune prétention d'exhaustivité. Nous omettrons ainsi volontairement d'opérer une distinction conceptuelle entre la valeur, la portée et les fonctions de la vie privée (par exemple : contrôle de l'information personnelle, protection de la dignité humaine, préservation de l'intimité, construction des relations sociales, restriction d'accès, etc.), exercice par ailleurs tout à fait réalisable dans un autre contexte.

[42] A. F. WESTIN, préc., note 1, p. 11. Westin écrit, aux pages 10-11 : « [w]hat the animal studies demonstrate is that virtually all animals have need for the temporary individual seclusion or small-unit intimacy […] In this sense, the quest for privacy is not restricted to man alone, but arises in the biological and social processes of all life ».

individuellement (1.1.1) et qu'elle assure la cohésion sociale nécessaire à toute existence en communauté (1.1.2).

1.1.1. La vie privée comme vecteur de réalisation individuelle

La question de l'importance de la vie privée fut l'objet, dans plusieurs domaines du savoir, d'une attention considérable[43]. Nous nous contenterons ici d'en esquisser les grandes lignes. Il est pertinent de préciser, d'entrée de jeu, que les caractéristiques d'une personne généralement considérées comme étant « privées » ne participent pas toutes de la définition de son individualité, pas plus qu'elles ne sont toutes centrales à sa vie ou à son bien-être (par exemple, son revenu), alors que d'autres, plus apparentes peuvent quant à elles s'avérer beaucoup plus importantes (par exemple, l'âge, l'origine ethnique, le statut familial, la profession, etc.)[44].

Néanmoins, toutes ces caractéristiques relèvent du domaine de la vie privée, et les fonctions que cette dernière permet d'exercer sont fondamentales à tout individu[45]. Certains

---

[43] Anita L. Allen rapporte, dans un aperçu de la question, que les chercheurs en sciences sociales ont conclu que des pratiques visant à protéger la vie privée étaient présentes dans virtuellement toutes les cultures humaines et fonctionnaient comme un mécanisme visant à limiter l'observation et le dévoilement et que, pour les philosophes et les théoriciens du droit, son respect était garant de la dignité humaine, de l'individualité et de l'harmonie en communauté, et qu'elle devait être appréhendée comme un droit moral fondamental. Voir Anita L. ALLEN, *Uneasy Access. Privacy for Women in a Free Society*, Totowa, Rowman & Littlefield, 1988, p. 35.

[44] Selon Ferdinand Schoeman, « [q]ualities such as age, race, family status, profession and general appearance are central to us even though we do not generally regard these as private. And other characteristics are taken as private even though they do not have much to do with what is central to our lives or with the integrity of our intimate selves, for example, annual income ». Ferdinand D. SCHOEMAN, « Privacy and intimate information », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 403, à la page 412.

[45] Sur ce point, Ruth Gavison énonce: « [...] my analysis of privacy suggests that the functions of privacy are [...] basic to human life ». Voir R. GAVISON, préc., note 29, 465.

auteurs ont avancé que la vie privée, de par son importance, aurait une valeur intrinsèque, donc inhérente à tout être humain, indépendamment des fonctions qu'elle permet à l'individu d'accomplir. À ce sujet, Ronald Dworkin considère, dans « A Matter of Principle », que l'absence de vie privée décisionnelle réduirait la capacité des individus, possédant un droit moral à l'égalité de respect et de considération, de mettre en jeu leurs propres idées relativement aux meilleures circonstances permettant la prospérité humaine[46]. Anita L. Allen estime pour sa part qu'il est primordial de promouvoir la vie privée puisqu'il s'agit d'une valeur « irreducibly worthy of respect »[47]. Dans une perspective plus contextuelle, Jeffrey H. Reiman avance que la vie privée est nécessaire à la création du « soi-même », en ce qu'elle permet aux individus de s'approprier leurs pensées, leur corps et leurs actions[48]. Dans le même ordre d'idées, Charles Fried énonce que la vie privée est essentielle afin d'assurer, chez l'individu, le développement de comportements de base tels que la confiance, l'amour et l'amitié[49]. Alan F. Westin estime quant à lui que la vie privée exerce, dans le cadre d'une société démocratique, quatre fonctions au bénéfice des individus, soit : favoriser l'autonomie personnelle, le relâchement émotionnel, l'auto-évaluation et limiter et protéger les communications[50]. Qui plus est, Westin affirme que, sans pour autant être une fin en soi, la vie privée constituerait un instrument permettant l'atteinte d'objectifs individuels de « self-realization »[51]. Dans tous ces cas, il apparaît clairement que la vie privée revêt une très grande importance dans la vie, le développement et le bien-être des individus.

---

[46] C'est ce qui ressort de l'analyse des propos de Anita Allen, dans A. L. ALLEN, préc., note 43, p. 39.
[47] *Id.*, p. 37.
[48] Jeffrey H. REIMAN, « Privacy, Intimacy and Personhood », (1976) 6-1 *Phil. & Pub. Aff.* 26, 39.
[49] Charles FRIED, « Privacy », (1968) 77-3 *Yale L. J.* 475, 482 et 484.
[50] A. F. WESTIN, préc., note 1, p. 32-38.
[51] *Id.*, p. 39.

Il serait possible de présenter ici un nombre incalculable de cas de figure illustrant l'importance qu'est susceptible d'avoir la sphère privée dans l'existence individuelle de tout un chacun. Qu'il nous suffise de dire que la protection d'un espace privé est fondamentale au développement équilibré de tout individu. Participe de ce développement l'élaboration ou l'articulation progressive des idées, des perceptions et des opinions spécifiques à chacun. Il en va de même de l'expérience profonde et sincère de toute émotion, que les invididus désirent instinctivement bien souvent expérimenter en solitude ou dont ils désirent généralement limiter la diffusion. Sur cet aspect – comme sur bien d'autres –, la vie privée participe d'un processus de limitation et de contrôle individuel des informations personnelles et des émotions. Ce contrôle inhérent à la moindre démarche temporaire, mais sporadiquement nécessaire, de réclusion dans l'espace privé rend possible toute réflexion approfondie sur quelque sujet que ce soit. Ce recul, fondamental à la prise de décision, permet aux individus de gouverner leur conduite à l'abri des influences externes non désirées[52]. En ce sens, la vie privée accorde ni plus ni moins aux individus la capacité de pondérer, dans l'intimité, leurs valeurs et attributs les plus intimes à la lumière des perceptions extérieures et, ce faisant, de progressivement développer leur personnalité et leur individualité. De cette manière, ils vivent « derrière un masque »[53]. Il ressort de cette brève présentation que la vie privée jouit d'une importance considérable relativement au développement du « soi » et de l'individualisation de chacun, conditions *sine qua non* à l'exercice d'une citoyenneté responsable dans toute société

---

[52] Sur cet aspect, Ruth Gavison énonce: « [p]rivacy [...] prevents interference, pressures to conform, ridicule, punishment, unfavorable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform them ». R. GAVISON, préc., note 29, 448.

[53] A. F. WESTIN, préc., note 1, p. 33. Selon Westin, « [e]very individual lives behind a mask [...]; indeed, the first etymological meaning of the word « person » was « mask », indicating both a conscious and expressive presentation of the self to a social audience ».

démocratique. Bien qu'indispensable à la vie dans une telle société, la protection de l'espace privé demeure, dans une très large mesure, complémentaire à l'espace public, en regard duquel il se définit. Ultimement, la réalisation individuelle, aussi importante soit-elle, ne peut être pleinement appréhendée qu'à la lumière du regard externe. Dans cet ordre d'idées, la vie privée permet également aux individus de coexister socialement et, à ce titre, elle constitue un important vecteur de cohésion sociale.

1.1.2. La vie privée comme vecteur de cohésion sociale

Il serait facile, voire tentant, dans une perspective strictement sociale, de concevoir la vie privée individuelle comme une valeur suspecte[54]. Néanmoins, l'appréhension de sa valeur pour la société nécessite qu'on la conçoive dans sa globalité, donc dans ses dimensions individuelles, aussi bien que sociales. Ainsi, le développement d'une personnalité propre, favorisé par la préservation d'une sphère privée individuelle, ne peut être adéquatement circonscrit que dans une perspective complémentaire, dans la mesure où il permet d'assurer une cohésion et une participation sociales nécessaires à toute vie démocratique digne de ce nom. Tout d'abord, l'émergence d'une autonomie personnelle individuelle, rendue possible par l'aménagement d'une sphère privée, constitue, d'un point de vue collectif, une condition indispensable à toute participation significative dans la gouvernance de la communauté et ses institutions, qu'elles soient politiques, économiques ou sociales[55]. Dans cette optique, la vie privée constitue l'une des caractéristiques les plus importantes de notre humanité et de notre

---

[54] F. D. SCHOEMAN, préc., note 15, à la page 403, où l'auteur avance: « [p]rivacy in itself is suspect as a value. It makes deception possible and provides the context for concealing things about which we may feel ashamed or guilty ».

[55] J. E. COHEN, préc., note 37, 1426.

civilisation[56]. La structuration de nos processus sociaux en est, selon nous, directement tributaire, notamment dû à la liberté d'action qu'elle procure aux individus. En plus de son effet structurant sur nos rapports sociaux, James Rachel considère qu'elle permet d'en aménager la portée, dans la mesure où elle permet aux individus d'ajuster leur comportement en fonction de l'identité des gens qui leur ont accès[57] et de la nature de leur relation. Ceci explique qu'un individu se comportera différemment avec son meilleur ami, son docteur, son patron ou encore sa belle-mère et, ce faisant, l'étendue et la manière de ce qu'il révèle sur lui-même seront appelées à varier. La vie privée permet ainsi l'établissement de rapports humains, lesquels participent indéniablement d'une vie enrichissante[58]. À ce titre, elle constitue, au sein des sociétés démocratiques occidentales, une valeur culturelle fondamentale[59]. La professeure Julie E. Cohen va même jusqu'à avancer qu'il s'agit d'un élément constitutif d'une société civile, dans le sens le plus large du terme[60]. De surcroît, la vie privée est, selon Ruth B. Gavison, porteuse d'une liberté d'action favorisant de nombreux objectifs, à savoir la capacité d'éviter la censure et le ridicule, la promotion de la santé mentale, de l'autonomie et des relations humaines, en plus de limiter l'exposition de l'individu[61]. Il appert donc que la vie privée revêt une importance considérable dans la structuration des rapports sociaux tels que nous les connaissons.

---

[56] Voir Thomas NAGEL, *Concealment and Exposure. And Other Essays*, Oxford, Oxford University Press, 2002, p. 4, où l'auteur avance que les bénéfices découlant de la vie privée sont fondamentaux à l'essence même de notre mode de vie civilisé: « [...] the importance of concealment as a condition of civilization. Concealment includes not only secrecy and deception but also reticence and non-acknowledgment. There is much more going on inside us all the time than we are willing to express, and civilization would be impossible if we could all read each other's minds. ».

[57] James RACHELS, « Why privacy is important », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 290, à la page 296.

[58] R. GAVISON, préc., note 29, 455.

[59] A. SCHAFER, préc., note 40, à la page 14.

[60] J. E. COHEN, préc., note 37, 1427-1428.

[61] R. GAVISON, préc., note 29, 448-455.

Tout comme dans le cas de son importance individuelle, les fonctions sociales que permet la préservation d'un espace privé sont fondamentales et les bénéfices collectifs découlant de celui-ci sont inestimables. Toujours dans une perspective complémentaire, le développement d'une individualité propre à chacun, telle que précédemment articulée, est aussi indispensable à la sauvegarde de la richesse de la vie démocratique qu'il ne l'est au bien-être de chaque citoyen. Cette individualité assure une relative préservation de l'intégrité nécessaire à toute contribution significative dans les processus sociaux et politiques inhérents à une société démocratique digne de ce nom. La vie privée permet, à ce titre, la pleine participation – du moins en théorie – des individus à la gouvernance démocratique et, par le fait même, garantit la plénitude de la joute politique contemporaine et en préserve la légitimité. Sur ce point, la vie privée serait essentielle à la gouvernance démocratique dans la mesure où elle favoriserait et encouragerait l'autonomie morale des citoyens, laquelle constitue un élément central de toute démocratie[62]. D'ailleurs, pour Priscilla M. Regan, la valeur publique de la vie privée serait liée à la valeur accordée à la dignité et à l'autonomie humaine[63], à son importance globale pour le système politique démocratique, notamment en ce qu'elle offrirait une protection permettant de restreindre l'arbitraire du pouvoir du gouvernement, mais également à son importance quant à la mise en commun de ce qui est nécessaire pour unir une communauté politique donnée[64]. Ce faisant, la vie privée est une valeur dont l'importance culturelle et sociale s'avère inestimable, ne serait-ce que parce qu'elle contribue à structurer et aménager la portée de nos rapports sociaux. Dans ce contexte,

[62] *Id.*, 455.

[63] Priscilla M. REGAN, « Privacy as a Common Good in the Digital World », (2002) 5-3 *Information, Communication & Society* 382, 399. Pour Regan: « [t]he common value of privacy derives in large part from a moral argument that privacy is intrinsically valuable as part of human dignity and autonomy ».

[64] *Id.* Sur ce dernier aspect, l'auteure parle du « development of commonality that is necessary to unite a political community ».

il est aisé de concevoir en quoi sa protection participe au maintien de la cohésion sociale indispensable à toute société démocratique. Finalement, bien qu'elle ne soit pas, à proprement parler, vitale à l'existence de l'humain au même titre que le sont l'air et l'eau, elle nous permet, selon Anita L. Allen, de gérer avec ce qui est nécessaire pour vivre en communauté[65].

En conclusion, bien qu'englobant deux aspects conceptuellement distincts, soit les sphères privée et publique, la vie privée constitue, en somme, un tout dont l'importance démocratique est fondamentale. Ruth Gavison résume bien la question, lorsqu'elle affirme que les raisons nous poussant à invoquer la protection de la vie privée dans différentes situations sont, ultimement, similaires, en ce qu'elles sont liées aux fonctions qu'exerce celle-ci dans nos vies : promouvoir la liberté, l'autonomie, l'individualité et les relations humaines, ainsi que favoriser l'existence d'une société libre[66]. Pour Anita L. Allen, deux généralisations sont possibles quant à l'importance de la vie privée : d'une part, les nombreuses formes de réclusion qu'elle permet ont plusieurs fonctions pratiques et, d'autre part, elle contribue à l'amélioration des individus et des relations qu'ils entretiennent, de telle manière qu'il soit impossible de les ignorer, dans une perspective éthique, pour quiconque considère que les individus ne devraient pas être traités comme de simples « choses »[67]. Qu'il s'agisse de ses fonctions premières et des bienfaits directs que peut en tirer chacun sur une base individuelle, ou encore de son importance structurelle primordiale et des nombreux bénéfices qui en

---

[65] A. L. ALLEN, préc., note 43, p. 1.

[66] R. GAVISON, préc., note 29, 423. L'auteure avance également, à la page 442, que de nombreuses et diverses valeures bénéficient de la protection de la vie privée: « [...] the values served by privacy are many and diverse. They include a healthy, liberal, democratic, and pluralistic society; individual autonomy; mental health; creativity; and the capacity to form and maintain meaningful relations with others ».

[67] A. L. ALLEN, préc., note 43, p. 52.

découlent le plan collectif et social, la vie privée participe activement à la définition du caractère démocratique de la société canadienne et, à ce titre, mérite d'être protégée.

Bien que nous n'ayons, à des fins de concision, pas spécifiquement traité de ce point, le caractère adéquat de cette protection est impératif quant à l'exercice de nombreux autres droits et libertés fondamentaux[68]. Nous n'avons, par exemple, qu'à penser aux libertés d'association, d'expression ou de conscience, ou encore au droit à la non-discrimination, dont l'exercice présuppose l'existence d'une protection juridique de la vie privée, sans quoi son effectivité deviendrait rapidement illusoire. Bref, il importe, dans une perspective théorique comme pragmatique, de préserver l'intégrité de la protection dévolue à la vie privée en regard des phénomènes contemporains susceptibles de contribuer à son érosion, à commencer par la surveillance électronique gouvernementale à grande échelle et la collecte des métadonnées. Cet enjeu est au cœur de la réflexion que nous proposons dans ce mémoire. Or, celle-ci implique que nous insistions, dans cette première partie, sur l'importance fondamentale de la vie privée en démocratie, ainsi que sur les risques que présentent la surveillance électronique gouvernementale à grande échelle et la collecte des métadonnées. Dans cet ordre d'idées, il nous semble nécessaire, avant de circonscrire l'étendue de la protection juridique dont bénéficie aujourd'hui la vie privée en droit canadien, puis d'approfondir notre réflexion, d'analyser la portée et l'intensité de la surveillance et de la collecte des métadonnées au Canada, de même que ses conséquences sur la vie privée.

---

[68] Priscilla M. Regan cite, lorsqu'elle aborde la valeur publique de la vie privée, son importance relativement à l'exercice de droits considérés comme étant essentiels à la démocratie, tels le droit à la liberté d'expression et le droit d'association. Voir P. M. REGAN, préc., note 63, 399; James Rachels considère pour sa part que la vie privée fait partie intégrante de la liberté. Voir J. RACHELS, préc., note 57, à la page 296.

1.2. La surveillance électronique gouvernementale et la collecte des métadonnées

Il fut démontré, dans la sous-partie précédente, que la vie privée revêtait une importance fondamentale pour les individus, comme pour la société, en plus de constituer une valeur cardinale de tout état démocratique digne de ce nom. Son primat au sein du régime des droits et libertés fondamentaux, de même que l'effectivité de sa protection, se trouvent aujourd'hui sérieusement remis en question, notamment à la lumière des activités de surveillance électronique gouvernementale des métadonnées[69]. Il est toutefois nécessaire, avant d'aborder la question centrale qui nous intéresse, à savoir celle de la protection juridique des métadonnées au Canada, de nous pencher sur le concept de métadonnée et de nous intéresser à la teneur et à l'ampleur de leur surveillance électronique. Cette démarche s'avère cruciale à la réflexion que nous proposerons dans la troisième partie de ce mémoire, ne serait-ce que pour bien situer les risques que présentent une protection juridique partielle des métadonnées et, par le fait même, évaluer la pertinence, voire la nécessité de proposer l'élaboration d'un cadre d'analyse alternatif à celui actuellement en vigueur[70]. Précisons d'ailleurs que cette sous-partie, à l'image du projet de mémoire dans son ensemble, vise uniquement les activités de surveillance opérées par des autorités gouvernementales occidentales sur leur propre territoire dans l'optique d'assurer la sécurité nationale. Incidemment, l'espionnage, dans toutes ses formes, qu'il soit interétatique, industriel ou autre, ainsi que le travail policier, tel qu'encadré par la procédure d'obtention de mandat, ne sont pas visés par notre réflexion. Bref, avant

---

[69] Il existe toute une gamme de phénomènes contemporains contribuant à mettre à mal le primat de la protection de la vie privée et son effectivité, dont il n'est pas dans notre intention de traiter. Nous n'aurions, par exemple, qu'à penser à la révélation volontaire d'informations sur les réseaux sociaux, au traitement et au partage des renseignements personnels au sein des entreprises privées, à l'avènement de l'interconnection des objets ménagers, à l'informatisation des systèmes jusqu'alors mécaniques, puis électroniques, tels que ceux contenus dans les véhicules automobiles, etc.

[70] *Infra*, partie III.

d'être en mesure de présenter la nature et l'ampleur des activités gouvernementales de surveillance électronique, particulièrement à l'égard des métadonnées, il importe, d'entrée de jeu, de déterminer précisément la signification du concept de métadonnée (1.2.1). Ce n'est qu'après nous être penché sur ce concept qu'il nous sera possible de traiter spécifiquement de la surveillance électronique des métadonnées (1.2.2).

1.2.1. Le concept de métadonnées et ses implications

L'une des premières réactions publiques des gouvernements occidentaux suite aux révélations, en juin 2013 par Edward Snowden, de l'existence de nombreux programmes de surveillance électronique à grande échelle des communications mondiales, fut d'insister sur le fait que ces programmes ne visaient généralement « que » les métadonnées des communications[71] interceptées[72]. Cette position se fonde sur la prémisse selon laquelle seul le contenu d'une communication est susceptible de présenter un intérêt réel pour la vie privée des individus dont les communications sont interceptées. Or, cette prémisse ne nous semble aujourd'hui plus valide, particulièrement face à la prédominance des technologies de l'information dans les sociétés occidentales industrialisées et à la prégnance des informations de toutes sortes dans nos vies quotidiennes. Nous reconnaissons toutefois que les assurances

---

[71] Pour les fins de ce mémoire, nous entendrons par « communication » les communications effectuées à l'aide d'un appareil téléphonique sans-fil de type « cellulaire » et celles effectuées par le biais d'un service de messagerie électronique informatisée.

[72] Pour la déclaration officielle du Président Barack Obama, voir Barack OBAMA, « Statement by the President », *The White House, Office of the Press Secretary* (juin 2013), en ligne : <http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president> (dernière consultation le 18 février 2015). Pour la déclaration de la Sénatrice Dianne Feinstein, voir Ed O'KEEFE, « Transcript: Dianne Feinstein, Saxby Chambliss explain, defend NSA phone records program », *The Washington Post* (juin 2013), en ligne : <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/> (dernière consultation le 18 février 2015).

selon lesquelles il ne s'agit « que » de métadonnées peuvent, à première vue, sembler raisonnables et fondées pour un public non initié aux technicités juridico-informatiques sous-tendant leur formulation. Il appert néanmoins manifeste, pour quiconque s'intéresse de plus près aux questions soulevées par les révélations de Snowden, que la surveillance des métadonnées présente de nombreuses implications, qu'elles soient juridiques, sociales ou politiques. Nous estimons donc pertinent, voire essentiel, de consacrer quelques précisions au concept de métadonnée avant de nous intéresser à la nature et à l'ampleur de leur surveillance. Ainsi, nous définirons ce concept (1.2.1.1), avant de traiter de la distinction existant entre le contenu et les métadonnées d'une communication (1.2.1.2), puis de l'importance qu'elles présentent dans notre ère caractérisée par l'omniprésence des données (1.2.1.3), avant de conclure sur ce qu'elles sont susceptibles de révéler à notre égard (1.2.1.4).

1.2.1.1. Les métadonnées : une définition

Le gouvernement du Canada définit les métadonnées comme étant des « donnée[s] relative[s] à des données ou à des éléments de données, y compris leurs descriptions de données, ou donnée[s] sur la propriété des données, les chemins d'accès, les droits d'accès et la volatilité des données »[73]. L'Office québécois de la langue française en fournit une définition plus brève, à savoir des « donnée[s] qui renseigne[nt] sur la nature de certaines autres données

[73] OTTAWA, TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *TERMIUM Plus*, « Métadonnée », 2011, en ligne : <http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=&index=alt&__index=alt&srchtxt=m%E9tadonn%E9e&comencsrch.x=0&comencsrch.y=0> (dernière consultation le 18 février 2015). Le Secrétariat du Conseil du Trésor du Canada les définit comme étant des « données qui définissent et décrivent d'autres données, et qui servent à identifier, à décrire, à localiser ou à utiliser les systèmes, les sources et les éléments d'information ». Voir OTTAWA, SECRETARIAT DU CONSEIL DU TRESOR DU CANADA, *Métadonnées*, 2012, en ligne : <http://www.tbs-sct.gc.ca/im-gi/imrc-crgi/metadata-metadonnees-fra.asp> (dernière consultation le 18 février 2015).

et qui permet[tent] ainsi leur utilisation pertinente »[74]. Dans une perspective mieux adaptée à la surveillance des communications électroniques, l'*American Civil Liberties Union* (ci-après, l'« ACLU ») réfère aux métadonnées comme étant « toute[s] donnée[s] autre[s] que le contenu d'une communication »[75]. Nous souscrirons à cette dernière conception aux fins de notre réflexion. Nous sommes tout à fait conscients que le concept de métadonnée peut sembler, même après avoir été défini, relativement abstrait. Pour cette raison, nous avons cru pertinent de concevoir et de présenter, à la page suivante, un tableau illustrant la nature des métadonnées générées, dans le cadre de l'utilisation, sur une base quotidienne, de trois services populaires :

---

[74] QUEBEC, OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2002, « Métadonnée », en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8869869> (dernière consultation le 18 février 2015).

[75] La version originale du texte énonce: « […] any data other than the contents of a communication ». Voir Chris CONLEY, *Metadata. Piecing Together a Privacy Solution*, San Francisco, American Civil Liberties Union of California, 2014, p. 3, en ligne : <https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf> (dernière consultation le 18 février 2015). Dans ce rapport fascinant, l'ACLU considère que la conception traditionnelle d'une métadonnée, soit une « donnée à propos d'une donnée » est, à la lumière de l'environnement technologique actuel – et tel que nous le verrons – beaucoup trop restrictive.

Tableau 1. Génération des métadonnées : un aperçu[76]		
Service utilisé	**Métadonnées générées**	
Courrier électronique	• Nom, adresse de courrier électronique et adresse IP de l'expéditeur • Nom et adresse de courrier électronique du destinataire • Information de transfert des serveurs • Date, heure et fuseau horaire • Identifiant unique du message électronique et des messages reliés • Type de contenu et encodage	• Données de connexion du client de messagerie grâce à l'adresse IP • Formatage des entêtes du client de messagerie • Priorités et catégories • Sujet du message électronique • État du message électronique • Demande de confirmation de lecture
Téléphonie cellulaire	• Numéro de téléphone de chaque participant à l'appel • Numéros de série uniques des téléphones utilisés • Heure de l'appel	• Durée de l'appel • Emplacement géographique de chaque participant à l'appel • Numéros de cartes téléphoniques
Twitter	• Nom, emplacement géographique, langue, information biographique contenue dans le profil et adresse URL • Date de création du compte • Nom d'utilisateur et identifiant unique • Emplacement, date, heure et fuseau horaire du « Tweet » • Identifiant unique du « Tweet » et de celui auquel l'utilisateur répondait	• Identifiants des contributeurs • Décompte du nombre de comptes « suivant » l'utilisateur, du nombre de comptes qu'il « suit » et de son nombre de « Tweets » favoris • Statut de vérification • Nom de l'application envoyant le « Tweet »

Il est important de garder à l'esprit que ces données sont, dans la très grande majorité des situations, générées sans même que l'utilisateur du service en question en ait conscience. Bref, il pourrait sembler aisé, à la consultation de ce tableau, de définir les métadonnées par ce qu'elles ne sont pas : du contenu. Néanmoins, la distinction entre les métadonnées et le contenu d'une communication n'est pas toujours aussi claire qu'elle y paraît à première vue.

[76] GUARDIAN US INTERACTIVE TEAM, « A Guardian guide to your metadata », *The Guardian* (juin 2013), en ligne : <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1000001> (dernière consultation le 18 février 2015). De nombreux autres appareils et services que nous utilisons sur une base quotidienne génèrent une impressionnante quantité de métadonnées, tels que notamment les navigateurs web, les moteurs de recherche, les sites de réseautage social (Facebook, etc.) et les appareils photographiques.

1.2.1.2. La distinction contenu-métadonnée

La distinction traditionnelle entre le contenu d'une communication et ses métadonnées est une question complexe. Ainsi, il n'existe pas, dans bien des situations, de séparation nette entre le contenu d'une communication et ses métadonnées alors que, dans d'autres circonstances, une information donnée peut être considérée, en fonction du contexte, aussi bien comme du contenu que comme une métadonnée[77]. Il en découle que la catégorisation appropriée d'une information dépend non seulement de son type, mais également du contexte dans lequel elle est créée ou utilisée[78].

Prenons, par exemple, le cas de l'information relative à l'emplacement d'un individu utilisant un téléphone cellulaire. L'emplacement de cet individu, à un moment donné, pourrait être déterminé à partir du contenu de sa communication ou encore des métadonnées générées par celle-ci. Dans le premier cas, l'information sur l'emplacement de l'individu, au moment de l'appel, serait expressément révélée dans le cadre de la conversation : il s'agirait de contenu. Dans le second cas, la même information pourrait également être révélée par la géolocalisation de l'appareil – et donc de l'individu – opérée par le fournisseur du service téléphonique au moment de l'appel : il s'agirait d'une métadonnée.

Michael Morell, anciennement directeur adjoint de la *Central Intelligence Agency*, relevait plus tôt cette année qu'il y a « dans » les métadonnées une importante quantité de contenu et qu'il n'existe pas, à proprement parler, de distinction marquée entre le contenu et

[77] C. CONLEY, préc., note 75, p. 3.
[78] *Id.*, p. 4.

les métadonnées d'une communication : il s'agirait plutôt d'un continuum[79]. Cette distinction « contenu-métadonnée » nous semble par ailleurs, dans une perspective juridique, beaucoup moins pertinente qu'auparavant. Il est vrai qu'elle pouvait sembler appropriée il y a plusieurs décennies, lorsque la technologie permettant de collecter et d'analyser les données était virtuellement inexistante, mais il est désormais impossible de prétendre que seul le contenu d'une communication puisse révéler des informations sensibles sur un individu[80]. Ce constat s'avère d'autant plus inquiétant si l'on considère la quantité pharaonique de données générées à chaque instant dans toutes les sphères de notre société numérique, y compris par les individus.

1.2.1.3. Les métadonnées à l'ère du « Big Data »

L'abondance de données et le rythme effarant auxquel elles sont aujourd'hui générées contribuent à exacerber les conséquences que présentent l'interception et l'analyse des métadonnées, dans une perspective quantitative aussi bien que qualitative[81]. Ceci étant, l'avènement récent du phénomène du « Big Data »[82] et, corrélativement, le développement et

---

[79] Julian SANCHEZ, « Obama Backs Off Real NSA Reforms », *The Daily Beast* (15 janvier 2014), en ligne : <http://www.thedailybeast.com/articles/2014/01/15/obama-backs-off-real-nsa-reform.html> (dernière consultation le 18 février 2015). Selon Michael Morell: « [t]here's a lot of content in metadata […] [t]here's not a sharp difference between metadata and content…It's more of a continuum ».

[80] C. CONLEY, préc., note 75, p. 2.

[81] Un nombre plus important de données signifie, quantitativement, plus d'informations à recueillir et permet, qualitativement, de tirer de ces données des inférences impossibles lors de l'analyse de données isolées.

[82] La quantité totale d'information disponible, sur la scène globale, en 2007, s'élevait à 295 exaoctets, soit l'équivalent de 404 milliards de CD-ROM de 730 mégaoctets. Voir Martin HILBERT et Priscila LÓPEZ, « The World's Technological Capacity to Store, Communicate, and Compute Information », (2011) 332 *Science* 60, 62. Dans la mesure où la quantité d'information numérique totale double tous les trois ans, Viktor Mayer-Schönberger et Kenneth Cukier avancent, suivant les travaux d'Hilbert, qu'elle s'élevait, en 2013, à 1 200 exaoctets, ce qui correspondrait à donner à chaque être humain une quantité d'information trois cent vingt fois plus importante que la somme d'information disponible dans l'ancienne bibliothèque d'Alexandrie. À ce sujet, voir V. MAYER-SCHÖNBERGER et K. CUKIER, préc., note 17, p. 9.

le raffinement d'un nombre toujours croissant de technologies analytiques, rend aujourd'hui possible l'analyse de ces quantités colossales de données recueillies. Cette analyse permet d'établir certaines corrélations entre un fait donné observé et la survenance future probable d'un autre fait déterminé[83]. Concrètement, les capacités technologiques actuellement disponibles rendent possible l'analyse efficiente des métadonnées recueillies, de manière à en faire émerger des modèles comportementaux précis concernant les utilisateurs responsables de l'émission desdites métadonnées[84].

À ce titre, le professeur Alex Pentland, du *Massachusetts Institute of Technology*, et Nathan Eagle ont démontré, dans une étude réalisée en 2004, que l'analyse des données émises par la fonction *Bluetooth* d'un téléphone cellulaire permettait l'identification de modèles comportementaux spécifiques, de même que la formulation d'inférences à propos du comportement futur de leurs utilisateurs[85]. De telles capacités s'avèrent d'autant plus

---

[83] V. MAYER-SCHÖNBERGER et K. CUKIER, préc., note 17, résument bien, à la page 53 de leur livre, le potentiel des « Big Data » en cette matière : « [b]y letting us identify a really good proxy for a phenomenon, correlations help us capture the present and predict the future : if A often takes place together with B, we need to watch out for B to predict that A will happen. Using B as a proxy helps us capture what is probably taking place with A, even if we can't measure or observe A directly. Importantly, it also helps us predict what may happen to A in the future. Of course, correlations cannot foretell the future, they can only predict it with a certain likelihood. But that ability is extremely valuable ».

[84] *Id.*, p. 90; et Robert LEE HOTZ, « The Really Smart Phone », *The Wall Street Journal* (avril 2011), en ligne : <http://online.wsj.com/news/articles/SB10001424052748704547604576263261679848814> (dernière consultation le 18 février 2015). Plus généralement, voir Wayne N. RENKE, « Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy », (2006) 43 *Alta. L. Rev.* 779.

[85] Nathan EAGLE et Alex PENTLAND, « Reality mining : sensing complex social systems », (2006) 10-4 *Personal and Ubiquitous Computing* 255. Les auteurs se prononcent également, à la page 256 de cette étude, sur le potentiel des téléphones cellulaires contemporains en matière de génération de données, de même que sur les implications soulevées relativement à la vie privée : « [o]utside the lab we envision a future where phones will have greater computational power and will be able to make relevant inferences using only data available to the user's phone. In this future scenario, the inferences are done in real-time on the local device, making it unnecessary for private information to be taken off the handset ». Dans le même ordre d'idées, voir également Nathan EAGLE, Alex PENTLAND et David LAZER, « Mobile Phone Data for Inferring Social Network Structure », dans Huan LIU, John J. SALERNO et Michael J. YOUNG (dir.), *Social Computing, Behavioral Modeling, and Prediction*, New York, Springer, 2008, p. 79 et s. Pour approfondir, voir Julia

inquiétantes, sur le plan juridique, que les métadonnées, de même que les modèles comportementaux que leur analyse permet d'appréhender, peuvent révéler autant, sinon plus d'information que le contenu d'une communication, et ce, particulièrement à la lumière de la quantité considérable de données de toutes sortes actuellement générées.

1.2.1.4. Le potentiel très révélateur des métadonnées

Selon l'ACLU, les métadonnées peuvent révéler notre identité, l'identité des gens que nous connaissons, ce que nous faisons et ce qui nous intéresse, ainsi que ce que nous planifions de faire : essentiellement le même spectre d'informations sensibles qui pourraient être révélées par l'analyse du contenu d'une communication[86]. Les métadonnées peuvent également révéler des informations qu'un individu n'a jamais eu l'intention de communiquer[87]. Il en découle que les métadonnées sont susceptibles de révéler un éventail d'informations de nature potentiellement privée sur les individus, bien souvent sans même que ces derniers n'en soient conscients, et ce, de plusieurs manières.

Tout d'abord, certaines métadonnées, prises individuellement, communiquent à leur face même, dû à leur nature, des informations intimes sur les individus[88]. C'est notamment le cas des informations qui nous permettent de savoir avec qui un individu communique, à quelle fréquence et pour combien de temps. Il serait, par exemple, aisé de déduire la confession religieuse d'un individu à partir du moment où il est établi qu'il est en contact régulier avec les

---

LANE, Victoria STODDEN, Stefan BENDER et Helen NISSENBAUM, *Privacy, Big Data, and the Public Good. Frameworks for Engagement*, Cambridge, Cambridge University Press, 2014.

[86] C. CONLEY, préc., note 75, p. 5.

[87] *Id.*

[88] *Id.*

représentants d'un lieu de culte local. De plus, certaines métadonnées peuvent révéler l'emplacement d'un individu – parfois même en temps réel, dans le cas d'un téléphone cellulaire – ce qui, encore une fois, implique la divulgation d'informations intimes, dans la mesure où l'emplacement d'un individu à un moment donné peut nous en apprendre beaucoup sur ses intérêts, ses convictions et ses occupations.

En deuxième lieu, les métadonnées, lorsqu'elles sont agrégées et forées[89], révèlent un nombre encore plus important d'informations potentiellement privées que lorsqu'elles sont analysées individuellement[90]. Ce serait, par exemple, le cas d'un individu qui, à l'intérieur d'une très courte période de temps, consulte un médecin omnipraticien, puis un dermatologue et, finalement, un oncologue, avant d'appeler à de multiples reprises les membres de sa famille les plus proches. Dans cette situation fictive – et à supposer que l'individu en question utilise exclusivement son téléphone cellulaire et le conserve généralement sur sa personne – l'agrégation et l'analyse des métadonnées de téléphonie cellulaire nous présenteraient un portrait assez représentatif de l'état de santé récent de l'individu visé.

En troisième lieu, certaines métadonnées peuvent révéler, avec un degré de certitude très élevé, l'identité d'un individu, même dans l'éventualité où elles sont anonymisées[91]. Ainsi, il est possible d'identifier quatre-vingt-quinze pour cent des individus grâce à seulement quatre marqueurs spatio-temporels anonymes, en l'occurence des médatonnées indiquant

---

[89] Nous référons ici à l'agrégation de données, ainsi qu'au forage de données (ou « Data Mining »), tel que traité précédemment. Voir *supra*, 1.2.1.3.
[90] C. CONLEY, préc., note 75, p. 6.
[91] *Id.*, p. 7.

l'emplacement d'un appareil de téléphonie cellulaire à un moment donné[92]. Cette analyse est rendue possible par le caractère tout à fait unique des habitudes de déplacement des individus, révélées par les métadonnées générées par leur appareil de téléphonie cellulaire[93].

En conclusion, nous sommes forcés de conclure que les métadonnées d'une communication sont, sous plusieurs aspects, très sensibles et peuvent s'avérer, à certains égards, plus révélatrices que le contenu de ladite communication. Ce potentiel qu'ont les métadonnées de révéler une myriade d'informations individuelles potentiellement privées ne devient toutefois réellement problématique, dans le contexte de notre réflexion[94], qu'à la lumière de l'intensité des activités gouvernementales dévolues spécifiquement à leur collecte et à leur surveillance à grande échelle.

---

[92] Yves-Alexandre DE MONTJOYE, César A. HIDALGO, Michel VERLEYSEN et Vincent D. BLONDEL, « Unique in the Crowd : The privacy bounds of human mobility », (2013) 3-1376 *Scientific Reports* 1, 1-3.

[93] *Id.*

[94] Nous reconnaissons toutefois d'emblée que les renseignements personnels présentent également, pour les institutions non-gouvernementales, un intérêt considérable. La collecte, le stockage et le partage de renseignements personnels à des fins commerciales et financières soulèvent d'ailleurs de très nombreuses – et urgentes – questions, que nous n'avons pas l'intention d'aborder dans le cadre de ce mémoire. Nous n'aurions par exemple qu'à penser aux défis théoriques et conceptuels qu'implique la protection de la vie privée informationnelle dans le contexte commercial, au sein d'une communauté en réseau. À ce titre, voir J. E. COHEN, préc., note 37. Qui plus est, nous aurions pu traiter, sur une base plus concrète, de la surveillance des consommateurs. À cet effet, voir David LYON, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis, University of Minnesota Press, 1994, p. 136-157; et Jason PRIDMORE, « Consumer surveillance. Context, perspectives and concerns in the personal information economy », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 321. Nous aurions également pu aborder la question de la surveillance à des fins publicitaires. Sur ce point, voir Joseph TUROW, « Cracking the Consumer Code : Advertisers, Anxiety, and Surveillance in the Digital Age », dans Kevin D. HAGGERTY et Richard V. ERICSON (dir.), *The New Politics of Surveillance and Visibility*, Toronto, University of Toronto Press, 2006, p. 279. Nous aurions finalement pu nous pencher sur la surveillance des utilisateurs des réseaux sociaux sur Internet. À ce sujet, voir Fernanda BRUNO, « Surveillance and participation on Web 2.0 », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 343. Il va sans dire que ces exemples ne se veulent pas représentatifs des multiples facettes de la surveillance privée. Bref, malgré l'importance fondamentale, la gravité et les dangers soulevés par ces enjeux, nous n'incorporerons pas la dimension privée de la collecte des renseignements personnels à notre mémoire, dans la mesure où son traitement impliquerait un raisonnement tout à fait différent du nôtre, lequel nous semble, au final, très peu susceptible de contribuer à l'élaboration de notre réflexion.

1.2.2. La surveillance électronique

Maintenant que nous avons défini le concept de métadonnée et cerné l'importance et le caractère privé de ce que leur analyse est susceptible de révéler, il est crucial de se pencher sur la surveillance gouvernementale à laquelle elles sont soumises, ne serait-ce que pour mettre en évidence les risques que présentent ces activités de surveillance en regard du droit à la vie privée. Précisons, tout d'abord, que les pratiques de surveillance ont, de tout temps, joué un rôle essentiel dans la stratégie gouvernementale de lutte contre la criminalité. C'est notamment le cas des moyens et techniques relevant de ce qu'il est aujourd'hui convenu d'appeler l'écoute, voire la surveillance électronique. Les autorités gouvernementales américaines et canadiennes ont par ailleurs eu recours à des techniques s'y apparentant durant la majeure partie du XX[e] siècle, tant aux États-Unis[95] qu'au Canada[96]. Ces techniques semblent en fait avoir présenté un tel attrait aux yeux des autorités que leur utilisation précède, du moins au Canada, leur encadrement juridique au niveau national[97]. Avant de traiter plus en détail de la

---

[95] PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, *The Challenge of Crime in a Free Society*, Washington, D.C., United States Government Printing Office, 1967, p. 202-203, en ligne : <https://www.ncjrs.gov/pdffiles1/nij/42.pdf> (dernière consultation le 18 février 2015).

[96] COMITE CANADIEN DE LA REFORME PENALE ET CORRECTIONNELLE, *Rapport du Comité canadien de la réforme pénale et correctionnelle. Justice pénale et correction : un lien à forger*, Ottawa, Imprimeur de la Reine pour le Canada, 1969, p. 89, en ligne : <http://www.johnhoward.ca/media/%281969%29%20HV%208395%20A6%20C33%201969%20F%20%28Ouimet%29.pdf> (dernière consultation le 18 février 2015); David A. CORNFIELD, « The Right to Privacy in Canada », (1967) 25 *U.T. Fac. L. Rev.* 103, 105-106.

[97] Il fallut, au Canada, attendre 1974 avant que ces techniques ne soient juridiquement encadrées au plan criminel, et ce, bien qu'elles constituaient un outil de première importance pour les autorités policières depuis longtemps. Voir Nathan FORESTER, « Electronic Surveillance, Criminal Investigations, and the Erosion of Constitutional Rights in Canada: Regressive U-Turn or a Mere Bump in the Road Towards Charter Justice? », (2010) 73 *Sask. L. Rev.* 23, 36 et s. Dans cette optique, le Comité canadien de la réforme pénale et correctionnelle (ci-après, le « Comité ») rapportait, en 1969, que l'« écoute clandestine au moyen du téléphone et d'appareils électroniques, dans le but de faire respecter la loi », n'était jusque là soumise à « aucun contrôle efficace » et, s'inspirant du droit américain, le Comité a recommandé que cette forme d'interception soit législativement autorisée et encadrée (COMITE CANADIEN DE LA REFORME PENALE ET CORRECTIONNELLE, *Rapport du Comité canadien de la réforme pénale et correctionnelle. Justice pénale et correction : un lien à forger*, Ottawa, Imprimeur de la Reine pour le Canada, 1969, p. 92, en ligne : <http://www.johnhoward.ca/media/%281969%29%20HV%208395%20A6%20C33%201969%20F%20%28

surveillance électronique des métadonnées, nous évacuerons les précisions terminologiques qu'implique toute réflexion sur les enjeux de surveillance (1.2.2.1), puis nous nous pencherons sur le phénomène d'intensification des activités de surveillance dans la foulée des attentats du 11 septembre 2001 (1.2.2.2). Nous serons, par la suite, en mesure de nous consacrer plus spécifiquement à la surveillance électronique des métadonnées (1.2.2.3) et au cas particulier du Canada (1.2.2.4).

1.2.2.1. La surveillance : quelques précisions terminologiques

Sans pour autant nous étendre sur ce point, force est de reconnaître que le concept de surveillance est lourd de signification, aussi bien dans ses dimensions politique et sociale qu'opérationnelle. Nous estimons donc nécessaire, d'une part, de définir le concept général de surveillance (1.2.2.1.1) et, d'autre part, de préciser le sens que nous accorderons au concept de surveillance électronique (1.2.2.1.2)

1.2.2.1.1. La surveillance

Historiquement, la surveillance visait, dû à la limitation des capacités technologiques, une dimension physique plutôt qu'électronique. Dans cet ordre d'idées, le Comité canadien de la réforme pénale et correctionnelle a défini, en 1969, la surveillance physique comme étant

---

Ouimet%29.pdf> (dernière consultation le 18 février 2015). Ainsi, l'article 802 du *Omnibus Crime Control and Safe Streets Act of 1968*, 42 U.S.C., § 3711, encadrait, selon le Comité, « l'interception, au moyen de quelque dispositif électronique, mécanique ou autre, de communications par fil ou de communications orales » (rapport du Comité, p. 91). En 1974, le Parlement canadien adopta, afin de donner suite aux observations du Comité sur ce point (énoncées aux pages 92 et suivantes du rapport du Comité), la *Loi sur la protection de la vie privée*, L.C. 1973-74, c. 50, amendant le *Code criminel*, L.R.C. 1985, c. C-46, de par l'ajout d'une nouvelle partie sur la protection de la vie privée, laquelle encadrait les activités relevant de notre conception contemporaine de la surveillance électronique.

« [l'acte de] repérer une personne que l'on soupçonne de se livrer à une activité criminelle, à la suivre, à observer ses actes et à surprendre ses conversations avec d'autres personnes »[98]. Stanley A. Cohen a avancé plus généralement, en 1982, que la surveillance pouvait être définie comme une activité impliquant l'observation d'individus, le rassemblement ou la collecte d'information à propos de ceux-ci ou en leur possession, ou encore l'interception de leurs communications[99]. Plus récemment, le Professeur David Lyon, à l'avant-scène des travaux dans le domaine émergent des *Surveillance Studies*, a formulé une définition plus inclusive de la surveillance, dans toutes ses dimensions, à savoir : « [surveillance] is the focused, systematic, and routine attention to personal details for purposes of influence, management, protection or direction »[100]. Ces trois définitions illustrent parfaitement le principe selon lequel les informations sont au cœur de toute démarche de surveillance, quelle qu'en soit sa forme. La surveillance électronique n'y fait pas exception.

1.2.2.1.2. La surveillance électronique

La surveillance électronique découle, logiquement et conceptuellement, de la surveillance dite « traditionnelle ». À ce titre, elle ne constitue qu'un outil spécialisé dont l'utilisation se confond, en pratique, avec les techniques physiques de surveillance, lesquelles participent toutes deux de la même dynamique de surveillance axée sur la collecte d'informations. Elle en diffère néanmoins à plusieurs égards, notamment de par le fait qu'elle est, par nature, plus élaborée et en ce qu'elle implique l'utilisation de procédés et de dispositifs

---

[98] COMITE CANADIEN DE LA REFORME PENALE ET CORRECTIONNELLE, préc., note 96, p. 86.
[99] Stanley A. COHEN, « Invasion of Privacy : Police and Electronic Surveillance in Canada », (1982) 27-4 *R.D. McGill* 619, 647.
[100] David LYON, *Surveillance Studies. An Overview*, Cambridge, Polity Press, 2007, p. 14.

technologiquement plus complexes. Selon James G. Carr, la surveillance électronique vise tout moyen par lequel une tierce partie, assistée d'un instrument électrique ou électronique, surprend une conversation entre deux autres individus[101]. David Watt adopte toutefois une approche plus englobante, dans la mesure où il considère qu'elle réfère à tout moyen permettant à un tiers de surprendre clandestinement, au moyen de tout appareil électromagnétique, acoustique, mécanique ou autre, une communication orale ou télécommunication entre deux individus ou plus[102]. Le concept de surveillance électronique dépasse toutefois depuis longtemps – et de très loin – la simple interception téléphonique au moyen d'un dispositif externe: il inclut également notamment, selon Nathan Forester, le recours aux dispositifs de repérage, aux enregistreurs de numéros de téléphone et à la surveillance vidéo[103].

Nous considérerons donc, aux fins du présent mémoire, que la notion de surveillance électronique vise tout moyen ou procédé, qu'il soit mécanique, acoustique, électronique ou autre, par lequel un tiers intercepte une communication orale ou écrite, ainsi que toute information y étant associée, entre deux individus ou plus[104]. Il va sans dire que les activités gouvernementales visant la surveillance, l'interception et la collecte des communications numériques et téléphoniques personnelles à des fins de sécurité tombent sous le champ d'application de cette définition. Bref, sans pour autant être fondamentalement différente de la

---

[101] James G. CARR, *The Law of Electronic Surveillance*, New York, Clark Boardman Company, 1977, p. 2.
[102] David WATT, *Law of Electronic Surveillance in Canada*, Toronto, Carswell, 1979, p. 12.
[103] N. FORESTER, préc., note 97, 24.
[104] Bien qu'à notre connaissance aucune disposition législative ne définisse expressément, au Canada, la notion de surveillance électronique, notre définition abonde dans le même sens que la définition d'« interception » d'une communication prévue au *Code criminel*, préc., note 97. En ce sens, le paragraphe 184(1) définit l'interception comme étant le fait « [d'intercepter volontairement], au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, […] une communication privée ».

surveillance physique, la surveillance électronique se distingue par sa forme, son caractère beaucoup plus envahissant et, incidemment, par le fait qu'elle soit plus difficile à cerner et à contrôler[105]. Ce caractère invasif et omniprésent ne saurait être illustré avec plus d'aplomb qu'à travers la présentation de la teneur des activités de surveillance étatique occidentales suivant les attentats terroristes du 11 septembre 2001.

1.2.2.2. L'accroissement de la surveillance post-11 septembre 2001

Il est désormais établi que l'étendue et l'ampleur des pratiques de surveillance de toute nature se sont considérablement accrues au sein des démocraties occidentales, y compris au Canada, depuis les évènements tragiques du 11 septembre 2001. Nous concentrerons toutefois exclusivement notre propos sur la dimension électronique de ces activités. Ceci étant, il est essentiel, afin de comprendre le rôle du gouvernement canadien quant à la surveillance électronique et à la collecte à grande échelle des métadonnées, de tout d'abord nous intéresser aux activités de notre plus important partenaire international en matière de sécurité – et chef de file en matière de surveillance électronique – les États-Unis d'Amérique. À cet effet – et nous y reviendrons – les activités de surveillance électronique du Canada et des États-Unis sont intimement liées au sein du réseau des *Five Eyes*[106].

---

[105] S. A. COHEN, préc., note 99, 643.

[106] Initialement établi en mars 1946 entre les États-Unis et le Royaume-Unis, le UK-USA Security Agreement fut élargi à trois autres partenaires du Commonwealth britannique en mai 1955, soit le Canada, l'Australie et la Nouvelle-Zélande. Pour plus d'information, voir NATIONAL SECURITY AGENCY, *UKUSA Agreement Release 1940-1956*, en ligne : <https://www.nsa.gov/public_info/declass/ukusa.shtml> (dernière consultation le 18 février 2015), ainsi que le texte de l'accord original amendé: ÉTATS-UNIS, ROYAUME-UNI, CANADA, AUSTRALIE et NOUVELLE-ZELANDE, TOP SECRET, *Amendment no. 4 to the appendices to the UKUSA Agreement*, LSIB/141/55, 1955, en ligne : <https://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf> (dernière consultation le 18 février 2015).

Il mérite par ailleurs d'être précisé qu'avant même les attentats du 11 septembre 2001, la *National Security Agency* (ci-après, la « NSA »), avec la collaboration de ses partenaires des *Five Eyes*, opérait déjà une importante surveillance des signaux électromagnétiques, notamment grâce au tristement célèbre – et massif – programme ECHELON[107]. Les méthodes dites « électroniques » de surveillance et de collecte d'informations se sont toutefois raffinées et répandues à un rythme soutenu en réponse aux attentats du 11 septembre 2001 en sol américain et conséquemment à l'accroissement des capacités et à la démocratisation des nouvelles technologies des communications. Bien qu'une telle démarche pourrait s'avérer très éclairante, il n'est pas dans notre intention de présenter ici de manière exhaustive les très nombreux programmes de surveillance électronique à grande échelle mis en place par la NSA et ses partenaires des *Five Eyes* ou par d'autres agences gouvernementales américaines depuis les attentats de septembre 2001[108], pas plus que de traiter, ne serait-ce que brièvement, de

---

[107] Duncan CAMPBELL, « Inside Echelon : The History, Structure, and Function of the Global Surveillance System Known as Echelon », dans Thomas Y. LEVIN, Ursula FROHNE et Peter WEIBEL (dir.), *CTRL [Space]. Rhetorics of Surveillance from Bentham to Big Brother*, Cambridge, The MIT Press, 2002, p. 158 aux pages 158-169; Armand MATTELART, *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, La Découverte, 2007, p. 74-75 et 167; et Torin MONAHAM, « Surveillance and terrorism », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge handbook of surveillance studies*, New York, Routledge, 2012, p. 285, à la page 285. Le New York Times rapportait déjà, en 2000, que le programme ECHELON visait l'interception et l'analyse des données satellitaires télévisuelles, Internet et vocales, ainsi que des télécopies : Tom ZELLER, « Ideas & Trends; Cloak, Dagger, Echelon », *The New York Times* (16 juillet 2000), en ligne : <http://www.nytimes.com/2000/07/16/technology/ideas-trends-cloak-dagger-echelon.html> (dernière consultation le 18 février 2015).

[108] Par exemple, le programme Total Information Awareness, opéré par l'*Information Awareness Office* en 2003, visait à prédire toute activité terroriste en permettant le partage et le forage d'un nombre considérable de types de données individuelles privées sur les citoyens américains, en les réorganisant et les centralisant au sein d'une base de données unique. Pour plus d'informations, voir le document de présentation original, tel qu'archivé : DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, « Total Information Awareness (TIA) System », en ligne : <http://web.archive.org/web/20021003053651/http://www.darpa.mil/iao/tiasystems.htm> (dernière consultation le 18 février 2015). Voir également UNITED STATES DEPARTMENT OF DEFENSE'S TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, *Safeguarding Privacy in the Fight Against Terrorism*, 2004, en ligne : <http://epic.org/privacy/profiling/tia/tapac_report.pdf> (dernière consultation le 18 février 2015). Le programme *PRISM*, opéré par la NSA depuis 2007, vise quant à lui à fournir à la NSA un accès direct aux serveurs informatiques de certains des plus grands opérateurs Internet, tels que Google, Yahoo, Apple et Facebook. Grâce à ce programme, la NSA est en mesure de collecter notamment l'historique de navigation

l'ensemble des mesures législatives visant à lutter contre le terrorisme adoptées au Canada[109] et aux États-Unis[110] en réponse à ces attentats. Qu'il nous suffise toutefois de préciser que, depuis le 11 septembre 2001, l'accroissement des activités gouvernementales de surveillance électronique, tant en termes de portée que d'intensité, fut considérable.

Il appert du travail journalistique mené notamment par Glenn Greenwald, dans la foulée des révélations du lanceur d'alertes Edward Snowden, que cet accroissement témoigne d'un changement de philosophie opérationnelle majeur relativement à l'ampleur, à la portée et à l'intensité des activités gouvernementales de surveillance électronique nécessaire à la prévention du terrorisme[111]. Le Général Keith B. Alexander, directeur de la NSA de 2005 à

---

des utilisateurs, le contenu de leurs messages, leurs photos et vidéos, les données stockées et la messagerie en temps réel. Pour plus d'information, voir Glenn GREENWALD et Ewen MACASKILL, « NSA Prism program taps into user data of Apple, Google, and others », *The Guardian* (juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (dernière consultation le 18 février 2015).

[109] Ainsi, le Canada adopta notamment, en décembre 2001, la *Loi antiterroriste*, L.C. 2001, c. 41, dont le préambule annonçait qu'elle avait pour objectif de « prévenir et supprimer le financement, la préparation et la commission d'actes de terrorisme et à protéger la sécurité nationale ». Le ministère de la Sécurité publique et de la Protection civile fut créé en 2003, puis la *Loi sur le ministère de la Sécurité publique et de la Protection civile*, L.C. 2005, c. 10, fut adoptée en 2005. Dans la foulée, le Gouvernement du Canada révéla, en 2004, le premier énoncé global en matière de sécurité nationale de l'histoire du pays : CANADA. BUREAU DU CONSEIL PRIVE, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Ottawa, Bureau du Conseil privé, 2004, en ligne : <http://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf> (dernière consultation le 18 février 2015). Pour plus d'information sur la politique sécuritaire du Canada post-11 septembre 2001, voir Elinor C. SLOAN, *Security and Defence in the Terrorist Era*, 2e éd., Montréal, McGill-Queen's University Press, 2010, p. 78 et s.

[110] Le Congrès américain adopta notamment, dès octobre 2001, le *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272, mieux connu sous son titre abrégé, à savoir le « Patriot Act ». À ce sujet, voir Richard FALK, « Encroaching on the Rule of Law. Post-9/11 Policies within the United States », dans Alison BRYSK et Gershon SHAFIR (dir.), *National Insecurity and Human Rights. Democracies Debate Counterterrorism*, Berkeley, University of California Press, 2007, p. 14 aux pages 34-36. Le United States Department of Homeland Security fut quant à lui créé en 2002 lors de l'adoption, par le Congrès américain, du *Homeland Security Act of 2002*, Pub. L. No. 107-296, 116 Stat. 2135. Pour plus d'information sur la politique sécuritaire des États-Unis post 11 septembre 2001, voir E. C. SLOAN, préc., note 109, p. 67 et s.

[111] À ce sujet, voir Glenn GREENWALD, « The crux of the NSA story in one phrase: "collect it all" », *The Guardian* (15 juillet 2013), en ligne : <http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all> (dernière consultation le 18 février 2015); et Glenn GREENWALD, « Glenn Greenwald: The

2014, aurait d'ailleurs personnellement affirmé qu'il était nécessaire, à des fins préventives, de « tout collecter »[112]. C'est dans cette optique que nous aborderons désormais la surveillance électronique et la collecte gouvernementale à grande échelle des métadonnées.

1.2.2.3. La surveillance électronique des métadonnées

Nous ne traiterons ici que des activités – pour l'essentiel américaines – de surveillance électronique à grande échelle visant spécifiquement les métadonnées et dont l'existence fut révélée en juin 2013, suite aux divulgations d'Edward Snowden. À cette occasion, nous apprenions notamment qu'en 2001, la NSA a procédé à la mise en place du programme *STELLARWIND*, qui visait à collecter et surveiller à grande échelle les métadonnées associées à l'utilisation d'Internet et de la messagerie électronique par les citoyens américains[113]. Une partie des activités de ce programme, officiellement abandonné en 2011[114], fut intégrée, dès

---

NSA's 'collect it all' mission », *National Post* (2 mai 2014), en ligne : <http://fullcomment.nationalpost.com/2014/05/02/glenn-greenwald-the-nsas-collect-it-all-mission/> (dernière consultation le 18 février 2015).

[112] Le Washington Post rapportait, en juillet 2013, dans un profil du général Keith B. Alexander, alors directeur de la NSA : « " [r]ather than look for a single needle in the haystack, his approach was, 'Let's collect the whole haystack,' " said one former senior U.S. intelligence official who tracked the plan's implementation. " Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it. " […] In his eight years at the helm of the country's electronic surveillance agency, Alexander, 61, has quietly presided over a revolution in the government's ability to scoop up information in the name of national security. And, as he did in Iraq, Alexander has pushed hard for everything he can get: tools, resources and the legal authority to collect and store vast quantities of raw information on American and foreign communications » (nos soulignements). Pour plus d'information, voir Ellen NAKASHIMA et Joby WARRICK, « For NSA chief, terrorist threat drives passion to 'collect it all' », *The Washington Post* (juillet 2013), en ligne : <http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html> (dernière consultation le 18 février 2015).

[113] Glenn GREENWALD et Spencer ACKERMAN, « NSA collected US email records in bulk for more than two years under Obama », *The Guardian* (juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama> (dernière consultation le 18 février 2015). Cette collecte « générale » n'était soumise à l'obtention d'aucun mandat spécifique, mais seulement à un processus de renouvellement trimestriel par un juge de la United States Foreign Intelligence Surveillance Court.

[114] *Id.*

2011, au programme *SHELLTRUMPET*, lancé en 2007 et visant à analyser en temps réel les métadonnées collectées par la NSA[115]. D'autres programmes intégrèrent les activités du défunt *STELLARWIND*, notamment les programmes *MAINWAY* et *MARINA*, qui visent respectivement le stockage et l'analyse des métadonnées téléphoniques et Internet collectées[116]. Les métadonnées ainsi interceptées et stockées par la NSA sont partagées avec 23 entités gouvernementales américaines distinctes exerçant des activités de renseignement, grâce à un moteur de recherche sophistiqué développé par la NSA et dénommé *ICREACH*[117]. La NSA est par ailleurs en mesure, grâce au programme *BOUNDLESS INFORMANT*, de procéder quotidiennement au décompte du nombre exact d'appels et de messages électroniques qu'elle intercepte et collecte partout à travers le monde, à savoir des milliards[118]. Bien que notre réflexion porte exclusivement sur le droit canadien, la présentation de ces programmes américains[119] contribue à mettre en évidence le fait que les métadonnées

---

[115] Glenn GREENWALD, *Nulle part où se cacher*, Paris, JC Lattès, 2014, p. 144-145. Glenn Greenwald y écrit – document officiel à l'appui – que la NSA se félicitait, en décembre 2012, d'avoir traité son trillionnième relevé de métadonnées, dont la moitié en 2012 uniquement. Voir également Glenn GREENWALD et Spencer ACKERMAN, « How the NSA is still harvesting your online data », *The Guardian* (27 juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection> (dernière consultation le 18 février 2015).

[116] Barton GELLMAN, « U.S. surveillance architecture includes collection of revealing Internet, phone metadata », *The Washington Post* (15 juin 2013), en ligne : <http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_print.html> (dernière consultation le 18 février 2015).

[117] Ce programme permet le partage de plus de 850 milliards de dossiers de métadonnées, incluant celles générées par des appels effectués à l'aide d'un téléphone cellulaire ou encore par des messages électroniques. Voir Ryan GALLAGHER, « The Surveillance Engine: How The Nsa Built its Own Secret Google », *The Intercept* (25 août 2014), en ligne : <https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/> (dernière consultation le 18 février 2015).

[118] G. GREENWALD, préc., note 115, p. 134-135.

[119] Cette présentation n'entretient aucune prétention d'exhaustivité. Il existe de nombreux autres programmes contemporains de surveillance électronique à grande échelle dont nous ne traiterons pas dans ce mémoire. Nous n'aurions, par exemple, qu'à penser au programme MUSCULAR, opéré conjointement par la NSA et le Government Communications Headquarters britannique et qui vise l'interception et la collecte des données personnelles contenues sur les serveurs de Google et Yahoo. À ce sujet, voir Barton GELLMAN et Ashkan SOLTANI, « NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say », *The Washington Post* (30 octobre 2013), en ligne : <http://www.washingtonpost.com/world/national-security/nsa-

présentent une valeur opérationnelle considérable dans le cadre des activités gouvernementales de surveillance à des fins de sécurité nationale. Ceci étant, il nous semble raisonnable de croire que le gouvernement du Canada puisse également s'intéresser, dans une perspective de renseignement de sécurité, aux métadonnées. Plusieurs facteurs nous permettent de le croire.

1.2.2.4. Le cas du Canada

Rappelons, d'entrée de jeu, et tel qu'il fut précédemment mentionné, que le Canada fait partie intégrante du réseau des *Five Eyes*, qui a pour objectif d'assurer la collaboration rapprochée de ses membres en matière de collecte et de partage de renseignements de sécurité. Dans ce cadre, le Centre de la sécurité des télécommunications du Canada (ci-après, le « CST »)[120] est appelé à collaborer très étroitement avec la NSA. Un document de la NSA encadrant la coopération entre les deux organisations, daté d'avril 2013, souligne que l'agence américaine offre au CST des « évolutions technologiques, des capacités de cryptologie, des logiciels et ressources pour une collecte de pointe, des moyens de traitement et d'analyse et des capacités en architecture informatique »[121]. En contrepartie, le CST offre à la NSA des «

---

infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> (dernière consultation le 18 février 2015).

[120] Le Centre de la sécurité des télécommunications, qui relève du ministère de la Défense nationale du Canada, a essentiellement pour mandat d'« acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers […] [de] fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada [et de] fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité », en vertu de l'article 273.64 de la *Loi sur la défense nationale*, L.R.C. 1985, c. N-5.

[121] Le document en question, classifié « TOP SECRET », est reproduit intégralement dans l'ouvrage de G. GREENWALD, préc., note 115, p. 172-173.

ressources de collecte avancée, de traitement et d'analyse […][,] des produits de cryptographie, de crypto-analyse, de haute technologie et des logiciels »[122].

Plus spécifiquement, le *Globe and Mail* rapportait, en juin 2013, que le ministre de la Défense nationale avait réapprouvé, en 2011, un programme de surveillance planétaire des métadonnées – incluant potentiellement celles de Canadiens – initialement mis en place en 2005[123]. Ce document soulève toutefois plus de questions qu'il n'apporte de réponses quant à l'intensité, à la portée et à la nationalité des individus visés par le programme de surveillance des métadonnées du CST, notamment en ce qui a trait aux métadonnées générées en territoire canadien[124]. Précisons, par ailleurs, qu'il n'est pas dans notre objectif de démontrer hors de tout doute raisonnable l'existence de programmes canadiens de surveillance électronique et de collecte à grande échelle des métadonnées, pas plus que de nous intéresser à l'encadrement législatif des activités de surveillance et de renseignement au Canada, notamment eu égard aux

---

[122] *Id.*

[123] Colin FREEZE, « Data-collection program got green light from MacKay in 2011 », *The Globe and Mail* (juin 2013), en ligne : <http://www.theglobeandmail.com/news/politics/data-collection-program-got-green-light-from-mackay-in-2011/article12444909/> (dernière consultation le 18 février 2015). L'autorisation ministérielle fait toutefois état de l'existence de mesures visant à protéger la vie privée des canadiens dont les métadonnées seraient captées par le programme, conformément notamment aux paragraphes 273.64(2) et (3), de même qu'aux paragraphes 273.65(1) à (5) de la *Loi sur la défense nationale*, L.R.C. 1985, c. N-5. Pour plus d'information, voir la demande d'autorisation originale et l'autorisation ministérielle, divulguées en vertu de la *Loi sur l'accès à l'information*, L.R.C. 1985, c. A-1 et publiées intégralement par le Globe and Mail : Colin FREEZE, « Raw documents : Canada's 'top secret' data mining program », *The Globe and Mail* (juin 2013), en ligne : <http://www.theglobeandmail.com/news/national/raw-documents-canadas-top-secret-data-mining-program/article12446852/?from=12444909> (dernière consultation le 18 février 2015).

[124] Le Professeur Craig Forcese, de l'Université d'Ottawa, pose ainsi une des questions qui nous apparaît des plus brûlantes à ce sujet: « [w]hat is the scope of the metadata directive -- does it truly relate to « every phone call and every Internet-based communication carried out by a Canadian »? If so, then it is almost certainly ultra vires the competence of CSEC, and there is a big problem ». Voir Craig FORCESE, « Metastasized Metadata: More On The CSEC Ministerial Authorization », *National Security Law Blog* (12 juin 2013), en ligne : <http://craigforcese.squarespace.com/national-security-law-blog/2013/6/12/metastasized-metadata-more-on-the-csec-ministerial-authoriza.html> (dernière consultation le 18 février 2015).

pouvoirs du CST et à ses limites[125]. Le CST semble, à tout le moins, conscient du caractère sensible que présente la surveillance des métadonnées[126].

Bref, il n'en demeure pas moins que les métadonnées, dû aux informations qu'elles permettent d'inférer sur l'identité, la vie et le comportement des individus, présentent selon nous un intérêt opérationnel certain pour le CST. Sans pour autant être en mesure de le prouver, il existe à nos yeux des motifs raisonnables, tels qu'entre autres la volonté politique de prévenir le terrorisme à tout prix et la disponibilité de capacités technologiques considérables, nous amenant à croire que certaines activités gouvernementales de surveillance électronique à grande échelle pourraient viser, de manière volontaire ou accidentelle, aujourd'hui ou dans un futur rapproché, des métadonnées générées en territoire canadien. Ainsi, il nous apparaît très fortement improbable que la surveillance à grande échelle des métadonnées, incluant celles générées sur le territoire national, soit une pratique exclusive de la NSA, particulièrement lorsque l'on considère l'importance de ces données, la nature des programmes de surveillance mis en place par la NSA depuis 2001, de même que la proximité

---

[125] Il existe, au niveau fédéral, de nombreuses lois encadrant, à divers aspects, la surveillance, qu'il s'agisse de la *Loi sur la défense nationale*, préc., note 120, la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, c. C-23, la *Loi sur la Gendarmerie royale du Canada*, L.R.C. 1985, c. R-10, ou encore du *Code criminel*, préc., note 97. Dans le même ordre d'idées – et toujours au niveau fédéral – les autorités policières sont notamment assujetties, dans le cadre de la collecte de renseignements personnels, à la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21; et la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

[126] Cette question est abordée de front sur le site Internet du CST, où l'on apprend qu'« [a]fin de réaliser son mandat, le CST recueille et analyse différentes sortes de métadonnées […] On ne retrouve pas de communications privées dans les métadonnées, mais il est possible de retrouver, dans quelques types de métadonnées, certains renseignements personnels. Par conséquent, comme en ce qui a trait à toutes les activités du CST, des mesures sont en place pour protéger la vie privée des Canadiens lorsque l'on traite des métadonnées dont l'auteur peut s'attendre à ce qu'elles ne soient pas interceptées ». Pour de plus amples informations, voir CENTRE DE LA SECURITE DES TELECOMMUNICATIONS, « Que fait le CST pour protéger la vie privée des Canadiens? », en ligne : <https://www.cse-cst.gc.ca/fr/page/que-fait-cst-proteger-vie-privee-canadiens> (dernière consultation le 18 février 2015).

du Canada et des États-Unis en matière de collecte et de partage de renseignements de sécurité.

En conclusion, il appert clairement de cette sous-partie que les métadonnées sont bien plus que de simples « données sur des données ». Sans pour autant directement relever du contenu d'une communication téléphonique ou Internet, elles s'y confondent fréquemment, en fonction de leur nature et, plus généralement, du contexte global dans lequel s'effectue une communication. Ceci étant, nous estimons que le maintien de la distinction conceptuelle et juridique ayant traditionnellement prévalu entre le contenu d'une communication et ses métadonnées est aujourd'hui difficilement justifiable. En effet, les inférences qu'il est possible de tirer de l'analyse de la surabondance de données quotidiennement générées par chaque individu rendent bien illusoire l'argument selon lequel seul le contenu d'une communication revêt un caractère privé. Ainsi, les métadonnées sont susceptibles de révéler une quantité impressionnante d'informations de nature privée sur un individu, notamment son identité, son emplacement, son orientation sexuelle, ses champs d'intérêt, son état de santé, ses affiliations, sa profession, ses activités ou ses appartenances religieuse et politique. Qui plus est, les métadonnées ne jouissent actuellement pas, en droit canadien – et tel qu'il sera démontré plus loin – d'une protection similaire à celle dont bénéficie le contenu d'une communication[127]. Cette situation s'avère d'autant plus inquiétante à la lumière de la portée des activités de surveillance électronique actuellement en place aux États-Unis et, dans une moindre mesure, possiblement au Canada. Finalement, il est indéniable que de telles activités de surveillance, de par leur nature même, sont susceptibles d'être problématiques à plusieurs égards,

[127] *Infra*, parties II et III.

particulièrement en ce qui concerne le droit à la vie privée[128], mais également en ce qui a trait au droit à la liberté d'expression[129].

Conclusion provisoire

La première partie de ce mémoire avait un double objectif. Elle visait tout d'abord à mettre en évidence l'importance fondamentale que revêt la vie privée dans la vie des individus et les fonctions essentielles qu'elle leur permet d'exercer au bénéfice de la collectivité. Dans cette perspective, nous avons d'abord souligné le rôle central qu'occupe, dans la vie de chacun, la préservation d'une sphère privée quant à l'élaboration et à l'articulation des idées, à l'expérience profonde des émotions, à l'expérimentation, de même qu'au développement de toute individualité. Comme nous l'avons explicité, ce processus de repli encourage l'autonomie morale des individus, ce qui leur permet de participer rationnellement aux interactions sociales et de pleinement exister, dans une dimension collective. Cette individualité assure, plus précisément, la possibilité de contribuer de manière originale, pertinente et significative aux processus politiques et sociaux, lesquels sont partie intégrante

---

[128] Dû au caractère intrinsèquement privé qu'elles revêtent, nous démontrerons plus loin dans ce mémoire qu'il pourrait être pertinent que les métadonnées d'une communication se voient conférer une protection juridique accrue.

[129] Le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression du Haut-Commissariat des Nations Unies aux droits de l'homme rapportait, en avril 2013, que : « [t|he right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect […] [T]he right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties ». Voir HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40, 23e sess., 2013, en ligne : <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement> (dernière consultation le 18 février 2015).

de toute démocratie digne de ce nom. La vie privée contribue donc concrètement à la réalisation de chaque individu, ainsi qu'à l'aménagement et à la structuration des rapports sociaux, participant par le fait même au maintien d'une relative cohésion sociale. Elle constitue, selon nous, une condition *sine qua non* à l'émergence et à la coexistence pérenne, sur une base sociétale, du « soi » et du « nous ».

Cette première partie visait également à mettre en évidence le risque d'atteinte à la vie privée et la gravité, pour l'individu comme pour la société, que présenterait la surveillance et la collecte à grande échelle des métadonnées générées par les communications téléphoniques et Internet des Canadiens. Pour ce faire, nous avons tout d'abord démontré que l'information contenue dans les métadonnées se confondait bien souvent, dans le contexte technologique actuel, avec le contenu des communications. Advenant le cas où il n'existe aucune confusion de ce type, les métadonnées peuvent tout de même révéler une quantité impressionnante d'informations de nature privée sur les individus, indépendamment du contenu des communications auxquelles elles sont associées. Il en découle que leur surveillance et leur collecte, par le biais de méthodes et techniques similaires à celles exposées dans cette première partie, entraveraient certainement la pleine protection que le droit se doit d'accorder, en démocratie, à la vie privée.

Finalement, il importe de préciser que nous souscrivons à une vision très réaliste de la lutte au terrorisme et au grave danger que les méthodes et tactiques de ces groupes présentent, notamment pour les institutions, infrastructures et populations occidentales. Nous reconnaissons la nécessité d'adopter une approche préventive et globale face à la menace

diffuse, opaque et omniprésente des activités menées par ces groupes terroristes de tout acabit. Il est donc indéniable que les moyens technologiques dont disposent les agences de renseignements occidentales, incluant la surveillance électronique des métadonnées, sont susceptibles de constituer un outil de premier plan dans cette lutte. L'ampleur et l'intensité de cette surveillance gouvernementale soulèvent néanmoins, dans leur forme actuelle, plusieurs questions quant au rôle du droit canadien et à sa capacité effective à régir, ne serait-ce que partiellement, les modalités de cette lutte au terrorisme. Ceci étant, le jeu démocratique occidental impose à tous – incluant les agences nationales de renseignement – le respect de certains principes et normes jugés fondamentaux à notre conception libérale de la démocratie moderne, tels que la primauté du droit, l'intégrité du processus judiciaire dans sa globalité et la protection des droits et libertés individuels. Il est d'ailleurs établi que la surveillance à grande échelle n'est pas sans conséquence pour les individus[130], pas plus qu'elle ne cadre avec notre conception de la démocratie[131]. La tendance actuelle visant, dans le milieu du renseignement, à « tout » collecter ne peut donc manquer d'induire de légitimes préoccupations, chez quiconque s'intéresse au rôle et à la place qu'occupent les droits et libertés fondamentaux au sein de

---

[130] Ainsi, le fait de savoir surveillé ou, ne serait-ce que la crainte de l'être, a pour conséquence directe d'altérer la manière dont les individus réfléchissent et se comportent. Sur ce point, voir A. F. WESTIN, préc., note 1, p. 57-63; Neil M. RICHARDS, « The Dangers of Surveillance », (2013) 126-7 *Harv. L. Rev.* 1934, 1945 et s.; et HUMAN RIGHTS WATCH et AMERICAN CIVIL LIBERTIES UNION, *With Liberty to Monitor All. How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*, Human Rights Watch, 2014, en ligne : <https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf> (dernière consultation le 18 février 2015). Concernant le rôle de l'appareil bureaucratique dans la mise en place des processus de surveillance et leur impact, voir C. DANDEKER, préc., note 16, p. 42-43. Concernant la collecte à grande échelle des données et ses impacts, voir W. N. RENKE, préc., note 84, 795 et s.; Lee TIEN, « Privacy, Technology and Data Mining », (2004) 30 *Ohio N. U. L. Rev.* 389, 399; et UNITED STATES DEPARTMENT OF DEFENSE'S TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, préc., note 108, p. 35-36.

[131] L'existence d'activités gouvernementales de surveillance à grande échelle, qu'elles soient physiques ou électroniques, est simplement conceptuellement incompatible avec notre vision libérale d'une démocratie occidentale et la protection effective des libertés individuelles qu'elle présuppose. À ce sujet, Julie E. Cohen avance qu'il est fort improbable qu'une société qui permet l'ascendance non encadrée des infrastructures de surveillance demeure une démocratie libérale. Voir Julie E. COHEN, « What Privacy is For », (2013) 126-7 *Harv. L. Rev.* 1904, 1912 et s.

l'ordre normatif canadien. La réflexion que nous proposons autour de la conception constitutionnelle du droit à la vie privée au Canada s'inscrit pleinement dans ce processus. Ainsi, pour assurer, en pratique, qu'il remplisse son rôle fondamental dans la vie des individus et l'aménagement démocratique des processus sociaux, il est impératif que le droit à la vie privée bénéficie d'une protection appropriée eu égard à l'ensemble des circonstances pertinentes. Bref, l'étendue et les capacités des activités contemporaines de surveillance électronique, conjuguées au caractère sensible des métadonnées, soulignent la pertinence de s'intéresser à leur place actuelle au sein du droit canadien, particulièrement au niveau constitutionnel. La seconde partie de ce mémoire sera consacrée à cet aspect de notre réflexion.

2. LA PROTECTION DU DROIT À LA VIE PRIVÉE AU CANADA

> *La loi, à l'origine, s'identifiait à cette frontière qui, autrefois, avait été en effet un espace, une sorte de no man's land entre le privé et le public, abritant et protégeant les deux domaines tout en les séparant l'un de l'autre.*
>
> Hannad Arendt[132]

Introduction

Il fut démontré, dans la première partie de ce mémoire, que la vie privée revêtait une importance fondamentale pour toute société démocratique telle que le Canada, de par les fonctions vitales qu'elle permet d'exercer, dans une dimension individuelle aussi bien que sociale. Nous avons donc vu qu'elle occupait une place centrale dans l'existence individuelle de tout un chacun, en plus d'être essentielle à l'organisation saine et rationnelle des processus sociaux. Il fut également démontré que les métadonnées générées par les communications effectuées par le biais d'un téléphone cellulaire ou d'un service de courrier électronique étaient susceptibles de révéler un nombre considérable d'informations à caractère privé sur les individus responsables desdites communications. Finalement, nous avons traité de l'ampleur de la surveillance électronique à laquelle certains gouvernements occidentaux, incluant le Canada, se livrent au nom de la lutte au terrorisme, notamment à l'égard des métadonnées des communications générées sur leur propre territoire.

À la lumière de l'importance qu'occupent aujourd'hui les communications effectuées par le biais d'un téléphone cellulaire ou d'un service de courrier électronique et du risque que

---

[132] H. ARENDT, préc., note 36, p. 104.

présentent les activités de surveillance électronique gouvernementales pour la vie privée, il nous semble crucial de poursuivre notre réflexion par le traitement des éléments juridiques pertinents à notre réflexion. Il en va de l'adaptation du droit national aux capacités technologiques contemporaines et, ultimement, de l'intégrité et de l'effectivité du cadre normatif prévoyant la protection du droit à la vie privée au Canada. La présente partie sera dévolue à la présentation de ce cadre normatif. Ainsi, nous traiterons tout d'abord, dans une optique positiviste, de l'étendue de la protection normative accordée à la vie privée en droit canadien, et ce, particulièrement dans sa dimension constitutionnelle (2.1). Par la suite, nous analyserons, plus en profondeur, la protection accordée à la vie privée informationnelle – dont relèvent les métadonnées d'une communication – en droit constitutionnel canadien, articulée autour du concept du « Biographical core » (2.2).

2.1. Le cadre normatif établi par le droit canadien

En raison de son importance pour les individus et pour la société, la vie privée bénéficie, en droit canadien, d'une protection juridique considérable, tant au niveau constitutionnel que statutaire. Cette sous-partie sera consacrée à cet aspect de notre réflexion. Ainsi, nous traiterons tout d'abord de la protection constitutionnelle de la vie privée prévue par la *Charte canadienne des droits et libertés* (1.2.1) puis, de manière accessoire, de la protection conférée par les lois statutaires pertinentes (1.2.2). L'accent sera mis, dans la présente sous-partie, sur la dimension constitutionnelle, dans la mesure où elle structurera notre traitement subséquent du cadre d'analyse propre à la vie privée informationnelle[133].

[133] *Infra*, sous-partie 2.2.

2.1.1. La protection constitutionnelle de la vie privée

Le juge La Forest a souligné, il y a plus de vingt-cinq ans, dans la désormais célèbre affaire *R.* c. *Dyment*[134], que la vie privée méritait d'être constitutionnellement protégée. Il considéra que cette protection était justifiée principalement pour deux raisons, à savoir son caractère essentiel au bien-être de l'individu, dans la mesure où elle est fondée sur son autonomie morale et physique, mais également parce qu'elle repose sur la limitation du pouvoir étatique de « s'intéresser de trop près à la vie des citoyens », principe au cœur de tout État démocratique[135]. Malgré cette importance fondamentale pour l'individu comme pour la société canadienne, la vie privée ne bénéficia pas toujours d'une protection juridique aussi importante qu'aujourd'hui. Le premier instrument juridique canadien de protection des droits de la personne au niveau fédéral, soit la *Déclaration canadienne des droits*[136], adoptée en 1960, n'accordait aucune protection directe au droit à la vie privée, et ce, bien qu'elle prévoyait un droit « à la vie, à la liberté [et] à la sécurité de la personne »[137]. La *Loi canadienne sur les droits de la personne*[138], adoptée en 1977, n'accorda quant à elle aucune protection au droit à la vie privée, se contentant d'interdire la discrimination dans les domaines de compétence fédérale.

---

[134] *R.* c. *Dyment*, [1988] 2 R.C.S. 417.
[135] *Id.*, par. 17.
[136] *Déclaration canadienne des droits*, L.C. 1960, c. 4.
[137] *Id.*, par. 1a). Cette formulation fut reprise, vingt-deux ans plus tard, à l'article 7 de la *Charte canadienne des droits et libertés*, puis interprétée par les tribunaux canadiens de manière favorable au droit à la vie privée, quoiqu'accessoirement à la protection directe dont bénéficie ce droit en vertu de l'article 8, depuis l'arrêt *Hunter* c. *Southam Inc.*, [1984] 2 R.C.S. 145. Voir *infra*, 2.1.1.1 et 2.1.1.2.
[138] *Loi canadienne sur les droits de la personne*, L.R.C. 1985, c. H-6.

La common law canadienne n'a, pour sa part, historiquement reconnu – et ne serait-ce qu'indirectement – qu'un faisceau d'intérêts analogues à la vie privée, principalement à travers la protection du droit de propriété[139]. Ce n'est seulement que lors de l'entrée en vigueur de la *Charte canadienne*, suivant le rapatriement de la Constitution en 1982, que le droit à la vie privée s'est vu accorder une protection constitutionnelle directe, qu'elle soit implicite et générale, par le biais de l'article 7, ou explicite et spécifique, par le biais de l'article 8[140].

2.1.1.1. L'article 7 de la Charte canadienne des droits et libertés

L'article 7 de la *Charte canadienne* prévoit ce qui suit :

> **7.** Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale.

Cet article protège les droits à la vie, à la liberté et à la sécurité et prévoit qu'il ne pourra leur être porté atteinte « qu'en conformité avec les principes de justice fondamentale ». La Cour suprême du Canada a dit de ces principes de justice fondamentale qu'ils « se trouvent dans les préceptes fondamentaux de notre système juridique [et qu'ils] relèvent non pas du domaine de l'ordre public en général, mais du pouvoir inhérent de l'appareil judiciaire en tant

---

[139] Voir notamment D. A. CORNFIELD, préc., note 96; Robert W. COSMAN, « A Man's House is his Castle – ''Beep'' : A Civil Law Remedy for the Invasion of Privacy », (1971) 29 *U.T. Fac. L. Rev.* 3; Philip H. OSBORNE, *The Law of Torts*, 4e éd., Toronto, Irwin Law, 2011; et Allen M. LINDEN et Bruce FELDTHUSEN, *Canadian Tort Law*, 9e éd., Markham, LexisNexis, 2011; Sans plus s'étendre sur la question de l'émergence d'une protection spécifique de la vie privée en common law, mentionnons seulement que la Cour suprême du Canada a souligné, depuis l'avènement de la *Charte canadienne*, l'importance du droit à la vie privée en common law. À ce sujet, voir les arrêts suivants: *R.* c. *Beare*, [1988] 2 R.C.S. 387 par. 110; *McInerney* c. *MacDonald*, [1992] 2 R.C.S. 138, 148-149; et *Hill* c. *Église de scientologie de Toronto*, [1995] 2 R.C.S. 1130.

[140] Nous ne traiterons pas de la *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, dans la mesure où notre réflexion sera exclusivement limitée à une dynamique de surveillance étatique, puisque le recours à une loi provinciale ne saurait nous être pertinent quant à l'interprétation d'un texte constitutionnel fédéral.

que gardien du système judiciaire »[141]. L'article 7 a donc essentiellement pour objet d'empêcher des atteintes à la vie, à la liberté et à la sécurité de la personne résultant d'une interaction de l'individu avec le système judiciaire et l'administration de la justice[142], dans la mesure où, comme nous venons de le préciser, de telles atteinte ne sont pas conformes aux principes de justice fondamentale. Cela étant, bien qu'elle soit d'une importance capitale, la justice fondamentale ne jouit d'aucune existence autonome : elle ne pourra être invoquée que dans la mesure où l'un des trois droits prévus à l'article 7 est en cause[143]. Une étude des droits pertinents de cet article – en l'occurrence les droits à la liberté et à la sécurité[144] – s'avère donc nécessaire à la compréhension adéquate de la protection conférée au droit à la vie privée par l'article 7, aussi limitée soit-elle. Notre analyse sera représentative du fait que la jurisprudence constitutionnelle en application de l'article 7 accorde une plus grande protection au droit à la vie privée à travers son traitement du droit à la liberté (1.2.1.1.1) que du droit à la sécurité (1.2.1.1.2).

2.1.1.1.1. La protection de la liberté : l'aménagement d'une sphère d'autonomie individuelle

Le lien entre l'article 7 et le droit à la vie privée découle d'une interprétation jurisprudentielle large du droit à la « liberté »[145], qui permet l'aménagement d'une sphère

---

[141] *Renvoi sur la Motor Vehicle Act (C.-B.)*, [1985] 2 R.C.S. 486, par. 31.

[142] *Nouveau Brunswick (Ministre de la Santé et des Services communautaires)* c. *G. (J.)*, [1999] 3 R.C.S. 46, par. 65. Tel qu'il fut précisé dans l'arrêt *Gosselin* c. *Québec (Procureur général)*, [2002] 4 R.C.S. 429, « la notion d'administration de la justice — et de façon plus générale la portée de l'art. 7 » sont susceptibles d'évoluer graduellement (par. 79).

[143] *Renvoi sur la Motor Vehicle Act (C.-B.)*, préc., note 141, 501; Henri BRUN, Guy TREMBLAY et Eugénie BROUILLET, *Droit constitutionnel*, 5e éd., Cowansville, Yvon Blais, 2008, p. 1100.

[144] Nous ne nous pencherons pas ici sur le droit à la vie puisque, bien que fondamental, il ne fut pas interprété par la jurisprudence comme accordant une quelconque protection spécifique au droit à la vie privée.

[145] *Singh* c. *Ministre de l'Emploi et de l'Immigration*, [1985] 1 R.C.S. 177, par. 43.

d'autonomie individuelle. Se fondant sur les propos du juge en chef Laskin dans l'affaire *R.* c. *Big M Drug Mart Ltd.*[146], la juge Wilson a énoncé, dans l'affaire *R.* c. *Morgentaler*, que « le droit à la liberté énoncé à l'art. 7 garantit à chaque individu une marge d'autonomie personnelle sur ses décisions importantes touchant intimement à sa vie privée »[147]. Ce principe fut réitéré par le juge La Forest, dans l'affaire *B. (R.)* c. *Children's Aid Society of Metropolitan Toronto*, lorsqu'il affirma que « dans une société libre et démocratique, l'individu doit avoir suffisamment d'autonomie personnelle pour vivre sa propre vie et prendre des décisions qui sont d'importance fondamentale pour sa personne »[148]. L'auteur Michael Power considère pour sa part que le lien le plus clair entre les concepts de liberté et de vie privée réside dans les propos du juge La Forest dans l'affaire *Godbout* c. *Longueuil (Ville)*[149], lorsqu'il écrit que « la protection du droit à la liberté garanti par l'art. 7 de la *Charte* s'étend au droit à une sphère irréductible d'autonomie personnelle où les individus peuvent prendre des décisions intrinsèquement privées sans intervention de l'État »[150].

Il va toutefois de soi que la liberté conférée par l'article 7 au nom de la protection d'un espace privé individuel n'implique pas pour autant, selon les Professeurs Brun, Tremblay et Brouillet, « le droit de faire n'importe quoi, sans avoir à subir quelque contrainte que ce soit de la part de

---

[146] *R.* c. *Big M Drug Mart Ltd.*, [1985] 1 R.C.S. 295. Selon le juge en chef, le caractère fondamental des libertés prévues à la *Charte canadienne* découle de l'importance de la valeur et de la dignité humaine et ces libertés constituent « le fondement même de la tradition politique dans laquelle s'insère la Charte» (par. 122).
[147] *R.* c. *Morgentaler*, [1988] 1 R.C.S. 30, par. 238.
[148] *B. (R.)* c. *Children's Aid Society of Metropolitan Toronto*, [1995] 1 R.C.S. 315, par. 80; Voir également *Blencoe* c. *Colombie-Britannique (Human Rights Commission)*, [2000] 2 R.C.S. 307, par. 49.
[149] Michael POWER, *The Law of Privacy*, Markham, LexisNexis, 2013, p. 232.
[150] *Godbout* c. *Longueuil (Ville)*, [1997] 3 R.C.S. 844, par. 66.

l'État »[151]. Ce principe, d'abord prévu dans l'arrêt *Morgentaler*[152], fut rappelé dans l'arrêt *Godbout*, dans lequel la cour précisa que :

> [L]'autonomie protégée par le droit à la liberté garanti par l'art. 7 ne comprend que les sujets qui peuvent à juste titre être qualifiés de fondamentalement ou d'essentiellement personnels et qui impliquent, par leur nature même, des choix fondamentaux participant de l'essence même de ce que signifie la jouissance de la dignité et de l'indépendance individuelles.[153]

Il en découle une importante limitation de la protection du droit à la vie privée au regard de l'article 7. Ce faisant, bien qu'ils constituent très certainement des éléments centraux de la notion de liberté, les intérêts que vise à protéger la vie privée ne sont pas absolus et, ultimement, ils doivent être pondérés par rapport aux intérêts concurrents de la société[154]. Bref, avant de traiter – brièvement – du lien entre le droit à la sécurité et la protection de la vie privée, il est possible de conclure, malgré son importante limitation, que le droit à la liberté, tel que prévu à l'article 7, prévoit « généralement [le droit] de jouir d'une vie privée »[155].

---

[151] H. BRUN, G. TREMBLAY et E. BROUILLET, préc., note 143, p. 1107.
[152] *R.* c. *Morgentaler*, préc., note 147, par. 228.
[153] *Godbout* c. *Longueuil (Ville)*, préc., note 150, par. 66; Concernant les balises de cette sphère d'autonomie, voir notamment les arrêts *Blencoe* c. *Colombie-Britannique (Human Rights Commission)*, préc., note 148; *Siemens* c. *Manitoba (Procureur général)*, [2003] 1 R.C.S. 6, par. 45; *R.* c. *Malmo-Levine; R.* c. *Caine*, [2003] 3 R.C.S. 571, par. 86; et *R.* c. *Clay*, [2003] 3 R.C.S. 735, par. 32-33.
[154] *R.* c. *O'Connor*, [1995] 4 R.C.S. 411, par. 130-132; M. POWER, préc., note 149, p. 233.
[155] H. BRUN, G. TREMBLAY et E. BROUILLET, préc., note 143, p. 1107.

2.1.1.1.2. La protection de la sécurité : le respect de l'intégrité individuelle

Il est également possible d'établir un lien entre l'article 7 et le droit à la vie privée de par l'interprétation jurisprudentielle du droit à la « sécurité ». Bien qu'elle soit beaucoup plus limitée qu'au regard du droit à la liberté, la protection conférée au droit à la vie privée par le droit à la sécurité implique la protection de l'intégrité physique individuelle. La juge McLachlin, se fondant sur l'arrêt de la Cour suprême dans l'affaire *Morgentaler*, considéra, dans l'affaire *Rodriguez* c. *Colombie-Britannique (Procureur général)*, que la protection du droit à la vie privée, à travers le droit à la sécurité, était intimement liée au droit à la liberté, en ce sens que « [l]a sécurité de la personne comporte un élément d'autonomie personnelle protégeant la dignité et la vie privée des individus à l'égard des décisions concernant leur propre corps »[156]. Le droit à la sécurité protège également l'intégrité psychologique des individus, laquelle est susceptible de comprendre, en fonction des circonstances, « l'atteinte à la vie privée »[157].

Finalement, nous sommes forcés de reconnaître que, malgré ce qui précède, l'article 7 de la *Charte canadienne* ne confère qu'une protection limitée au droit à la vie privée, à travers l'interprétation jurisprudentielle des fondements et de la portée des droits à la liberté et à la sécurité. Aucun des arrêts sur lesquels se fonde cette protection partielle ne prévoit ou n'établit de méthodologie juridique propre à encadrer l'analyse d'une éventuelle atteinte au droit à la

[156] *Rodriguez* c. *Colombie Britannique (Procureur général)*, [1993] 3 R.C.S. 519, 618. Bien que dissidente quant au raisonnement de la majorité, cet extrait réfère à des principes faisant l'unanimité au sein de la cour.
[157] *Mills* c. *La Reine*, [1986] 1 R.C.S. 863, par. 145.

vie privée aussi clairement en vertu de l'article 7[158] qu'en vertu de l'article 8. Bref, qu'il soit ou non directement constitutionnellement protégé par l'article 7, le droit à la vie privée est partie intégrante des intérêts protégés par les droits à la liberté et à la sécurité. L'analyse ici présentée visait à souligner l'importance générale du droit à la vie privée au sein de la *Charte canadienne*. Néanmoins, l'essentiel de la protection constitutionnelle dévolue à la vie privée en droit canadien est prévu par l'article 8, qui sera désormais analysé.

2.1.1.2. L'article 8 de la Charte canadienne des droits et libertés

L'article 8 de la *Charte canadienne* prévoit ce qui suit :

> 8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

L'article 8 a pour objet d'interdire les fouilles, les perquisitions ou les saisies abusives à l'échelle nationale, ce qui a pour effet d'accorder une protection considérable au droit à la vie privée. Alors que l'article 7 constituait une « clause générale de justice fondamentale », l'article 8, tout comme les articles 9 à 14, précise le sens à donner à ce concept de justice fondamentale sur certains points particuliers[159]. Ainsi, l'article 8 protège contre une atteinte spécifique au droit à la vie, à la liberté et à la sécurité prévu à l'article 7[160]. Il constitue une vibrante illustration de l'objectif général de la *Charte canadienne*, soit de « garantir et de protéger, dans des limites raisonnables, la jouissance des droits et libertés qu'elle enchâsse [et

---

[158] Barbara MCISAAC, Rick SHIELDS et Kris KLEIN, *The Law of Privacy in Canada*, Carswell, vol. 1, Toronto, 2000, p. 2-4.

[159] H. BRUN, G. TREMBLAY et E. BROUILLET, préc., note 143, p. 1098. Selon ces auteurs, les articles 8 à 14 seraient implicitement contenus dans l'article 7.

[160] *Renvoi sur la Motor Vehicle Act (C.-B.)*, préc., note 141, par. 28-29.

d']empêcher le gouvernement d'agir à l'encontre de ces droits et libertés »[161]. À ce titre, l'article 8 vise à « protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée »[162]. Cette protection participe d'une démarche globale de pondération des intérêts opposés, inhérente au processus de fouilles, perquisitions et saisies, tel que souligné par le juge en chef Dickson, dans l'arrêt *R.* c. *Genest* :

> Les intérêts en jeu sont primordiaux. D'un côté, on ne doit porter atteinte à la sécurité et au caractère privé de la maison et des possessions d'une personne que pour des motifs impérieux. Par ailleurs, la société, représentée par ses différentes institutions, a un intérêt incontestable et tout aussi vital à ce que le crime fasse l'objet d'enquêtes efficaces et à ce que les malfaiteurs soient punis. La tâche de soupeser ces intérêts opposés est d'une importance capitale et d'une difficulté considérable; mais il faut s'y essayer et, autant que possible, s'en acquitter adéquatement dans l'intérêt de la liberté civile et de l'application des lois.[163]

La protection aujourd'hui conférée à la vie privée par l'article 8 résulte d'un changement majeur de notre conception juridique de l'objet de la protection contre les fouilles, perquisitions et saisies abusives opéré à la fin des années 1960 aux États-Unis puis, près d'une vingtaine d'années plus tard, au Canada. Peter Hogg souligne que la protection de la vie privée a remplacé la protection des droits de propriété à titre de valeur consacrée par l'interdiction des fouilles, perquisitions et saisies abusives depuis l'arrêt de la Cour suprême des États-Unis dans l'affaire *Katz* v. *United States*[164], dans lequel la cour a jugé que « the fourth amendment protects people, not places »[165]. Au Canada, il fallut toutefois attendre l'avènement de la

---

[161] *Hunter* c. *Southam Inc.*, préc., note 137, 156.
[162] *Id.*, 160.
[163] *R.* c. *Genest*, [1989] 1 R.C.S. 59, 63; Suzanne BOUCHER et Kenneth LANDA, *Understanding Section 8 : Search, Seizure, and the Canadian Constitution*, Toronto, Irwin Law, 2005, p. 1-2. Voir également Steven PENNEY, « Unreasonable Search and Seizure and Section 8 of the Charter: Cost-benefit Analysis in Constitutional Interpretation », (2013) 62-2 *S.C.L.R.* 101, 101-104.
[164] *Katz* v. *United States*, [1967] 389 U.S. 347.
[165] *Id.*, 351. Le quatrième amendement de la Constitution des États-Unis, qui fait partie du *United States Bill of Rights*, U.S. Const., amend. I-X, prohibe les fouilles, perquisitions et saisies abusives et requiert que

Charte canadienne pour que ce principe soit repris puis intégré dans le droit par la Cour suprême du Canada, à l'occasion de la première affaire qu'elle entendit relativement à l'article 8, à savoir *Hunter* c. *Southam Inc.*[166]. Cette affaire portait essentiellement sur une contestation de la validité constitutionnelle de plusieurs dispositions de la *Loi relative aux enquêtes sur les coalitions*[167], qui permettaient au directeur des enquêtes et recherches de la direction des enquêtes sur les coalitions d'autoriser des fonctionnaires à pénétrer dans tout local où ce directeur croyait qu'il pouvait exister des preuves se rapportant à l'objet d'une enquête et à saisir celles-ci afin de les examiner plus en profondeur. Dans ce contexte, la cour énonça, d'entrée de jeu, qu'avant d'être en mesure d'évaluer « le caractère raisonnable ou abusif de l'effet d'une fouille ou d'une perquisition ou d'une loi autorisant une fouille ou une perquisition », il est nécessaire de cerner le but fondamental de l'article 8, soit – tel que nous l'avons précisé plus haut – de « protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée »[168]. Ce but implique que l'article 8 doive être interprété de manière à prévenir les atteintes, plutôt que de simplement y remédier, et que « la nature des droits qu'il vise à protéger » soit clairement délimitée[169]. Comme nous le verrons, ces droits sont limités par la notion d'« attente raisonnable »[170].

---

l'obtention de tout mandat soit fondée sur l'existence d'une justification sérieuse (« probable cause »). Voir Peter HOGG, *Constitutional Law of Canada*, 5e éd., vol. 2, Toronto, Carswell, 2007, p. 48-5.

[166] *Hunter* c. *Southam Inc.*, préc., note 137, 158-159. Avant cette affaire, l'interdiction des fouilles, perquisitions et saisies abusives reposait, en common law canadienne, sur la protection des droits de propriété. Quatre ans plus tard, la cour précisa, dans l'arrêt *R.* c. *Dyment*, préc., note 134 que « [l]'arrêt *Hunter* c. *Southam Inc.* a brisé les entraves qui limitaient ces revendications à la propriété […] ce qui est protégé, ce sont les personnes et non les lieux » (par. 20). Voir également P. HOGG, préc., note 165, p. 48-6.

[167] *Loi relative aux enquêtes sur les coalitions*, L.R.C. 1985, c. 19 (2e supp.). Anciennement S.R.C. 1970, c. C-23.

[168] *Hunter* c. *Southam Inc.*, préc., note 137, 160.

[169] *Id.*, 157.

[170] *Id.*, 159.

Bref, nous aborderons la nature et l'étendue de la protection constitutionnelle du droit à la vie privée en vertu de l'article 8 de la *Charte canadienne*, conformément à la démarche juridique proposée dans l'arrêt *Hunter* c. *Southam Inc*. Ainsi, nous nous concentrerons d'abord sur la détermination de l'existence d'une expectative de vie privée et son étendue, à travers l'étude du critère de l'attente raisonnable (1.2.1.2.1), pour ensuite traiter des modalités d'une violation de cette protection, à travers l'analyse du caractère raisonnable d'une perquisition, d'une fouille ou d'une saisie (1.2.1.2.2).

2.1.1.2.1. L'attente raisonnable en matière de vie privée

Le concept d'attente raisonnable en matière de vie privée constitue le fondement du cadre d'analyse de l'étendue de la protection constitutionnelle conférée au droit à la vie privée par l'article 8 de la *Charte canadienne*. Ainsi, nous établirons la structure et préciserons les principes essentiels dégagés par la jurisprudence constitutionnelle concernant l'objet de la protection du droit à la vie privée en vertu l'article 8[171]. Nous présenterons spécifiquement le critère de l'attente raisonnable, de même que l'analyse contextuelle que commande son application (1.2.1.2.1.1), avant d'aborder la question des différents intérêts protégés par le droit à la vie privée (1.2.1.2.1.2).

[171] L'analyse ici présentée sera limitée aux éléments directement pertinents à notre réflexion. Conséquemment, nous n'entretenons aucune prétention d'exhaustivité à l'égard des principes abordés et de leur traitement jurisprudentiel.

2.1.1.2.1.1. Le critère de l'« attente raisonnable »

Le critère de l'attente raisonnable en matière de vie privée constitue le cœur de l'analyse de la portée de l'article 8 de la *Charte canadienne*[172]. Ce critère témoigne du fait que la protection contre les fouilles, perquisitions et saisies abusives constitue essentiellement un « droit de s'attendre "raisonnablement" à la protection de la vie privée »[173]. Se fondant sur l'arrêt *Hunter* c. *Southam Inc.*, la Cour suprême a précisé, dans l'arrêt *R.* c. *M. (M.R.)*, qu'un individu désirant invoquer la protection de l'article 8 devait impérativement démontrer une attente raisonnable en matière de vie privée, à défaut de quoi il ne saurait y avoir de violation de l'article 8[174]. Cet article ne garantit donc un « droit général à la protection contre les fouilles ou perquisitions abusives [que] dans les cas où la personne qui en fait l'objet s'attend raisonnablement à ce que sa vie privée soit respectée »[175].

Cette attente raisonnable implique un exercice d'appréciation entre, d'une part, « le droit du public de ne pas être importuné par le gouvernement »[176] et, d'autre part, le « droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi »[177]. La Cour suprême s'est penchée à maintes reprises, durant les trois dernières décennies, sur ce processus d'appréciation des intérêts divergents et sur la signification appropriée à donner au concept d'attente raisonnable. Ainsi, il fut établi, dans l'arrêt *R.* c. *Wong*, que l'attente raisonnable en matière de vie privée ne

---

[172] B. MCISAAC, R. SHIELDS et K. KLEIN, préc., note 158, p. 2-17.
[173] *Hunter* c. *Southam Inc.*, préc., note 137, 159.
[174] *R.* c. *M. (M.R.)*, [1998] 3 R.C.S. 393, par. 31. Voir également *R.* c. *Edwards*, [1996] 1 R.C.S. 128; et *Schreiber* c. *Canada (Procureur général)*, [1998] 1 R.C.S. 841.
[175] *R.* c. *Wise*, [1992] 1 R.C.S. 527, 533.
[176] *Hunter* c. *Southam Inc.*, préc., note 137, 159.
[177] *Id.*, 160.

s'évaluait pas en regard d'une « notion générale du respect de la vie privée dans une société libre et démocratique dont une personne jouit en tout temps », mais bien plutôt à la lumière du contexte factuel particulier de chaque affaire[178]. Dans le même ordre d'idées, il fut jugé, dans l'affaire *R.* c. *Colarusso*, que l'analyse que commande l'article 8 de la *Charte canadienne* repose d'abord et avant tout sur la prise en compte du contexte particulier dans lequel s'exerce un pouvoir de fouille, de perquisition ou de saisie en question[179]. Toujours dans la même affaire, le juge La Forest a considéré que « le besoin de voir respecter sa vie privée [pouvait] varier selon la nature de ce qu'on veut protéger, les circonstances de l'ingérence de l'État et l'endroit où celle-ci se produit, et selon les buts de l'ingérence »[180].

Deux ans après son arrêt dans l'affaire Colarusso, la cour est allée encore plus loin, dans l'arrêt *R.* c. *Edwards* – qui demeure, jusqu'à aujourd'hui, l'arrêt de principe sur cette question – en précisant que « [l]'existence d'une attente raisonnable en matière de vie privée [devait] être déterminée eu égard à l'ensemble des circonstances » dans une situation donnée[181]. La cour a, par la suite, dressé une liste non exhaustive de facteurs à prendre en considération lors de l'appréciation de l'ensemble des circonstances, soit :

a. la présence du plaignant au moment de la perquisition;
b. la possession ou le contrôle du bien ou du lieu faisant l'objet de la fouille ou de la perquisition;
c. la propriété du bien ou du lieu;

---

[178] *R.* c. *Wong*, [1990] 3 R.C.S. 36, 61. Il en découle, par exemple, qu'un endroit normalement qualifié de lieu privé pourrait, en fonction de l'utilisation qui en est faite, devenir un lieu où une personne ne saurait s'attendre au respect de sa vie privée (p. 62).
[179] *R.* c. *Colarusso*, [1994] 1 R.C.S. 20, 38.
[180] *Id.*, 53.
[181] *R.* c. *Edwards*, préc., note 174, par. 45. Pour ce qui est de l'importance des circonstances eu égard au concept d'attente raisonnable en matière de vie privée, voir notamment les arrêts de la Cour suprême suivants : *R.* c. *Dyment*, préc., note 134, 431; *R.* c. *Wong*, préc., note 178, 62; *R.* c. *Colarusso*, préc., note 179, 54.

d. l'usage historique du bien ou de l'article;
e. l'habilité à régir l'accès au lieu, y compris le droit d'y recevoir ou d'en exclure autrui;
f. l'existence d'une attente subjective en matière de vie privée; et
g. le caractère raisonnable de l'attente, sur le plan objectif.[182]

Apportons quelques précisions sur ces deux derniers facteurs. D'une part, l'attente subjective réfère à la croyance qu'a un individu du caractère privé d'une situation donnée, qu'il s'agisse de son corps, d'un lieu ou d'une information. D'autre part, s'il existe une telle attente, il importera de se demander si elle est objectivement raisonnable, en regard d'un ensemble d'éléments particuliers, soit :

a. l'endroit où la prétendue « perquisition » a eu lieu;
b. si l'objet était à la vue du public;
c. si l'objet avait été abandonné;
d. si des tiers possédaient déjà les renseignements; dans l'affirmative, ces renseignements étaient-ils visés par une obligation de confidentialité?
e. si la technique policière a porté atteinte au droit à la vie privée;
f. si le recours à la technique de surveillance était lui-même déraisonnable d'un point de vue objectif;
g. si [l'information obtenue] a révélé des détails intimes sur le mode de vie de l'intimé ou des renseignements d'ordre biographique le concernant.[183]

Ces éléments réfèrent à la dimension objective de l'attente raisonnable en matière de vie privée. Il est ici fondamental de préciser que toute expectative raisonnable en matière de vie privée repose sur la présence cumulative de la dimension subjective de l'attente, à savoir la croyance qu'a un individu du caractère privé que présente une situation donnée, ainsi que de sa dimension objective, soit le caractère réellement privé de cette même situation, indépendamment de l'attente que peut avoir l'individu en question à cet effet. Qui plus est, la Cour suprême a établi, dans l'arrêt *R.* c. *Tessling*, que « l'attente en matière de vie privée est

[182] *R.* c. *Edwards*, préc., note 174, par. 45.
[183] *R.* c. *Tessling*, [2004] 3 R.C.S. 432, par. 32. Voir également *R.* c. *Patrick*, [2009] 1 R.C.S. 579, par. 26-27, où la cour se livre à un exercice de synthèse fort utile quant au raisonnement approprié à adopter eu égard à l'analyse de l'ensemble des circonstances.

de nature normative et non descriptive », ce qui signifie qu'une « diminution de l'attente *subjective* en matière de vie privée [ne] se traduira [pas] automatiquement par une diminution correspondante de la protection constitutionnelle »[184]. La prise en compte des dimensions subjective et objective s'avérera donc, dans chaque cas, cruciale.

Bref, la détermination de l'existence d'une attente raisonnable en matière de vie privée dépendra des faits de chaque espèce et toutes les circonstances de la fouille, la perquisition ou la saisie devront être rigoureusement prises en compte[185]. L'exercice d'appréciation globale que cette démarche implique est crucial, dans la mesure où les circonstances, facteurs et éléments pertinents de chaque cas sont susceptibles d'être interreliés et interdépendants, tel que l'a récemment mentionné la Cour suprême, dans l'arrêt *R.* c. *Spencer* :

> On détermine s'il existe une attente raisonnable en matière de respect de la vie privée, compte tenu de l'ensemble des circonstances, en examinant et en soupesant un grand nombre de facteurs interreliés qui comprennent à la fois des facteurs relatifs à la nature des droits en matière de vie privée visés par l'action de l'État et des facteurs qui ont trait plus directement à l'attente en matière de respect de la vie privée, considérée tant subjectivement qu'objectivement, par rapport à ces droits [.] La nécessité d'examiner ces éléments compte tenu de « l'ensemble des circonstances » fait ressortir le fait qu'ils sont souvent interdépendants, qu'ils doivent être adaptés aux circonstances de chaque cas, et qu'ils doivent être considérés dans leur ensemble.[186] (nos soulignements)

Il sera également nécessaire de tenir compte, lors de l'analyse de l'ensemble des circonstances, de la nature des revendications en matière de vie privée, lesquelles relèvent de

---

[184] *R.* c. *Tessling*, préc., note 183, par. 42.

[185] B. MCISAAC, R. SHIELDS et K. KLEIN, préc., note 158, p. 2-19. La Cour suprême a par ailleurs déterminé, dans l'arrêt *British Columbia Securities Commission* c. *Branch*, [1995] 2 R.C.S. 3, que la norme du caractère raisonnable serait interprétée différemment selon que la fouille, la perquisition ou la saisie survient en matière criminelle ou administrative et réglementaire (par. 52).

[186] *R.* c. *Spencer*, [2014] CSC 43, par. 17. Voir également le paragraphe 18.

trois domaines d'intérêts différents, voire de sphères, à savoir personnel (c.-à-d. corporel), territorial et informationnel.

2.1.1.2.1.2. Les intérêts protégés par la vie privée

Cette présentation des différents intérêts protégés par la vie privée sera très brève. Initialement théorisée dans le Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice intitulé *L'ordinateur et la vie privée*[187], la distinction entre les différents intérêts fut reprise par le juge La Forest, dans l'arrêt *R.* c. *Dyment*[188]. Ce faisant, nous traiterons successivement de la vie privée corporelle, puis territoriale, avant de rapidement présenter les grandes lignes de ce qui constitue la vie privée informationnelle, de laquelle découle le cadre d'analyse du « Biographical Core ». Précisons également que bien que la distinction entre les trois sphères d'intérêts constitue certes un outil d'analyse utile[189], celles-ci sont parfois appelées à se confondre et, par le fait même, à complexifier l'analyse du niveau approprié de protection de la vie privée dans une situation donnée[190].

En premier lieu, la vie privée corporelle concerne le niveau d'intimité que possède un individu sur son corps, ses effets et ses agissements. Elle est particulièrement pertinente dans le cas des fouilles corporelles effectuées par des agents gouvernementaux, qu'elles soient

---

[187] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, *L'ordinateur et la vie privée*, Ottawa, Information Canada, 1972, p. 12-15.
[188] *R.* c. *Dyment*, préc., note 134, par. 19.
[189] *R.* c. *Patrick*, préc., note 183, par. 42.
[190] Dans l'affaire *R.* c. *Tessling*, préc., note 183, la Cour d'appel de l'Ontario avait considéré que la captation d'images infrarouges d'une propriété privée relevait de la sphère territoriale, alors que la Cour suprême jugea qu'elle relevait de la sphère informationnelle.

simples (palpation superficielle, fouille manuelle, fouille à nu, etc.) ou plus complexes (radiographie, scanneur corporel, dispositif biométrique, etc.). Concrètement, elle protège le « droit de refuser toute palpation ou exploration corporelle qui dévoilerait des objets ou des matières qu'une personne veut dissimuler »[191]. Elle vise à sauvegarder la dignité humaine[192] et est intimement liée à notre conception sociétale de la décence et de l'intégrité corporelle[193], ce qui rend très grave toute violation de l'intégrité physique d'un individu dans le contexte de l'article 8[194]. L'attente raisonnable en matière de vie privée dans la sphère personnelle sera généralement très importante, dans la mesure où elle implique la protection et la préservation de cette intégrité[195]. Conséquemment, c'est cette dimension de la vie privée qui peut « le plus fortement prétendre à une protection constitutionnelle »[196]. Ce faisant, des auteurs avancent que l'interférence avec le corps humain se situe à l'extrémité supérieure du spectre des protections de la vie privée[197].

En deuxième lieu, la vie privée territoriale concerne le niveau d'intimité que possède un individu sur son environnement et ses possessions. Elle est particulièrement pertinente dans le cas des fouilles, perquisitions et saisies du milieu de vie et des biens d'un individu, quels que

---

[191] *Id.*, par. 21.

[192] *R.* c. *Dyment*, préc., note 134, par. 21; GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 13.

[193] Croft MICHAELSON, « The Limits of Privacy : Some Reflections on Section 8 of the Charter », (2008) 40-2 *S.C.L.R.* 87, 92.

[194] *R.* c. *Pohoretsky*, [1987] 1 R.C.S. 945, par. 5; *R.* c. *Dyment*, préc., note 134, par. 34; *R.* c. *Colarusso*, préc., note 179, 65 et 67; *R.* c. *Stillman*, [1997] 1 R.C.S. 607, par. 39 et 42; *R.* c. *Shoker*, [2006] 2 R.C.S. 399, par. 23.

[195] Sans pour autant traiter spécifiquement de cet aspect, il va sans dire que le niveau de protection de la vie privée dans le domaine personnel sera appelé à varier en fonction des circonstances et pourra, de ce fait, être considérablement réduit (par exemple, en prison, ou encore dans les forces armées, etc.).

[196] *R.* c. *Tessling*, préc., note 183, par. 21.

[197] S. BOUCHER et K. LANDA, préc., note 163, p. 37, où ils écrivent que « [the] [i]nterference with the human body is at one extreme end of the spectrum of privacy protections ».

soient leur forme ou leur niveau de complexité (fouille d'un véhicule automobile, entrée dans une maison d'habitation, installation de dispositifs de surveillance physique ou audiovisuelle sur une propriété, etc.). Cette dimension de la vie privée se rattache, dans une perspective historique, théorique et juridique, au concept de propriété[198] et vise à reconnaître l'existence d'un « domaine physique à l'intérieur duquel [l'individu dispose du] droit d'être seul et tranquille »[199]. Cet espace est assimilable à un « royaume privé » duquel l'individu est en mesure d'exclure autrui[200]. De plus, la protection juridique aujourd'hui accordée à certains lieux découle de la nature des interactions sociales qui s'y déroulent[201]. Dans les faits, il existe une « hiérarchie des lieux » protégés par l'article 8 de la *Charte canadienne*[202], la demeure y trônant au sommet[203]. Dans le même ordre d'idées, l'ensemble des circonstances d'une situation donnée, dont le contexte et la nature d'un bien, contribue à déterminer le niveau approprié de protection rattaché à la vie privée territoriale[204]. Mentionnons également que les violations de la vie privée touchant à la dimension territoriale sont, de l'avis de la Cour suprême, moins graves que celles impliquant la vie privée corporelle, ne serait-ce que parce qu'elles ne portent pas atteinte à l'intégrité physique de l'individu[205].

---

[198] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 13.
[199] *Id.*
[200] C. MICHAELSON, préc., note 193, 92-93.
[201] *R.* c. *Dyment*, préc., note 134, par. 20.
[202] *R.* c. *Tessling*, préc., note 183, par. 22.
[203] *Id.*; *R.* c. *MacDonald*, [2014] CSC 3, par. 26; *R.* c. *Godoy*, [1999] 1 R.C.S. 311, par. 19; *R.* c. *Feeney*, [1997] 2 R.C.S. 13; *R.* c. *Silveira*, [1995] 2 R.C.S. 297; et *R.* c. *Kokesch*, [1990] 3 R.C.S. 3.
[204] Par exemple, un terrain, un véhicule automobile, une chambre d'hôtel et une cellule de prison bénéficieront d'un niveau de protection différent.
[205] *R.* c. *Pohoretsky*, préc., note 194, par. 5.

En troisième lieu, la vie privée informationnelle concerne la protection dont jouit un individu relativement à ses informations personnelles et à ses communications. Cette dimension de la vie privée sera soulevée chaque fois que les actes de l'État, qu'il s'agisse de fouilles, perquisitions ou saisies, touchent aux informations ou aux communications privées d'un individu, quelle qu'en soit la méthode ou la portée[206]. Puisque la réflexion au cœur de ce mémoire est orientée précisément autour de la définition, des fondements et de la portée constitutionnelle de la vie privée informationnelle, nous en traiterons spécifiquement ultérieurement[207]. Contentons-nous toutefois dans l'immédiat de préciser qu'elle est conceptuellement plus complexe à appréhender et à délimiter que ne le sont les sphères corporelle et territoriale[208].

Finalement, ce n'est qu'une fois qu'un individu aura démontré qu'il peut raisonnablement s'attendre à la protection de sa vie privée, conformément aux conditions exposées plus haut – soit en fonction du contexte factuel, de l'ensemble des circonstances et de la nature des intérêts en question – qu'il sera possible d'évaluer le caractère raisonnable d'une fouille, perquisition ou saisie effectuée par le gouvernement en vertu de l'article 8 de la *Charte canadienne*.

---

[206] Il pourrait notamment s'agir, par exemple, des situations suivantes : fouille et analyse de documentation et de relevés comportant des informations personnelles, interception du contenu d'un appel téléphonique, surveillance des communications électroniques, surveillance des dispositifs électroniques et technologiques d'un individu, etc.

[207] *Infra*, sous-partie 2.2.

[208] Sur cette question de la délimitation entre les trois sphères privées, voir C. MICHAELSON, préc., note 193, 92-94.

2.1.1.2.2. Le caractère raisonnable d'une fouille, perquisition ou saisie : la violation de la protection conférée par l'article 8

Alors que nous nous sommes précédemment intéressés aux principes jurisprudentiels applicables à l'objet de la protection conférée à la vie privée par l'article 8 de la *Charte canadienne*, nous présenterons désormais les modalités applicables à la détermination du caractère raisonnable d'une fouille, d'une perquisition ou saisie.

D'entrée de jeu, la détermination de ce caractère raisonnable présuppose l'existence d'une attente raisonnable en matière de vie privée, faute de quoi les actes reprochés à l'État ne constitueront pas une « fouille, une perquisition ou une saisie » au sens de l'article 8 de la *Charte canadienne*[209]. La Cour suprême a jugé, dans l'arrêt *Hunter* c. *Southam Inc.*, que la détermination du caractère raisonnable d'une fouille, perquisition ou saisie, ou encore d'une loi l'autorisant, permettait d'en apprécier la constitutionnalité en fonction de leur effet « raisonnable » ou « abusif » relativement à l'objet de la fouille, perquisition ou saisie contestée[210]. Toujours selon la cour, cet exercice doit s'effectuer conformément au principe de prépondérance des droits au cœur de l'article 8, lequel vise à prévenir les fouilles, perquisitions ou saisies abusives avant qu'elles ne surviennent, grâce à « un système d'autorisation préalable et non de validation subséquente »[211] (soulignement original). Qui plus est, ce critère d'évaluation du caractère raisonnable doit être flexible, dans la mesure où il doit tenir compte non seulement du droit individuel à la vie privée et à la jouissance paisible de ses biens, mais également des considérations gouvernementales pratiques relatives à

[209] B. MCISAAC, R. SHIELDS et K. KLEIN, préc., note 158, p. 2-13; M. POWER, préc., note 149, p. 248.
[210] *Hunter* c. *Southam Inc.*, préc., note 137, 157.
[211] *Id.*, 160.

l'application de la loi[212]. C'est dans cette perspective que nous étudierons d'abord la détermination du caractère raisonnable d'une fouille, perquisition ou saisie (1.2.1.2.2.1), avant de traiter de l'exclusion des éléments de preuves recueillis en violation de l'article 8 (1.2.1.2.2.2).

2.1.1.2.2.1. La détermination du caractère raisonnable d'une fouille, perquisition ou saisie

La détermination du caractère raisonnable, donc non abusif, d'une fouille, perquisition ou saisie au regard de l'article 8 de la *Charte canadienne* s'effectue à la lumière de la méthode d'analyse développée par la Cour suprême dans l'arrêt *R.* c. *Collins* :

> Une fouille ne sera pas abusive si elle est autorisée par la loi, si la loi elle-même n'a rien d'abusif et si la fouille n'a pas été effectuée d'une manière abusive.[213]

Cette méthode d'analyse – ou test – prévoit donc trois étapes. Le respect de chacune d'elles est nécessaire pour conclure au caractère raisonnable d'une fouille, perquisition ou saisie. Ainsi, on devra tout d'abord déterminer si la fouille, perquisition ou saisie est autorisée par une loi ou par la common law[214]. Le non-respect de cette exigence aura pour conséquence de rendre la fouille, perquisition ou saisie illégale, ce qui suffit à la déclarer abusive[215].

On devra, par la suite, déterminer si la loi qui autorise la fouille, perquisition ou saisie n'a rien d'abusif, donc si elle est raisonnable. Pour ce faire, la loi devra respecter les exigences

---

[212] P. HOGG, préc., note 165, p. 48-4.
[213] *R.* c. *Collins*, [1987] 1 R.C.S. 265, par. 23.
[214] Voir *R.* c. *Caslake*, [1998] 1 R.C.S. 51, par. 12.
[215] La Cour suprême a précisé, au paragraphe 43 de l'arrêt *R.* c. *Dyment*, préc., note 134, que « [l]e fait que la saisie [soit] illégale […] répond à la question de savoir si la fouille était abusive ».

constitutionnelles établies dans l'arrêt *Hunter* c. *Southam Inc.*[216], soit prévoir un mécanisme d'autorisation préalable[217], dont l'appréciation est effectuée par une personne neutre et impartiale agissant judiciairement[218] et se fondant sur « l'existence de motifs raisonnables et probables, établie sous serment, de croire qu'une infraction a été commise et que des éléments de preuve se trouvent à l'endroit de la [fouille, perquisition ou saisie] »[219].

Finalement, on devra déterminer si la fouille, la perquisition ou la saisie a été menée de manière raisonnable. Encore une fois, l'ensemble des circonstances sera déterminant, notamment le caractère plus ou moins intrusif de la fouille, la méthode de surveillance employée et l'expectative plus ou moins grande entretenue par l'individu visé en matière de vie privée[220]. Précisons également que la surveillance électronique peut constituer une fouille, une perquisition ou une saisie aux fins de l'article 8[221]. Nous consacrerons désormais quelques mots à ce qu'il advient, concrètement, dans l'éventualité où une fouille, perquisition ou saisie ne remplit pas les trois conditions du test de l'arrêt *Collins*, dont nous venons de traiter.

2.1.1.2.2.2. La recevabilité des éléments de preuve

Précisons tout d'abord qu'une fouille déraisonnable – ou abusive – portant atteinte aux droits fondamentaux prévus à la *Charte canadienne*, en l'occurrence à l'article 8, ne sera pas

---

[216] Martin VAUCLAIR, « Fouilles et perquisitions: en saisir l'ampleur », dans S.F.P.B.Q., *Congrès annuel du Barreau du Québec (2003)*, Cowansville, Yvon Blais, 2003, p. 27, à la page 38.
[217] *Hunter* c. *Southam Inc.*, préc., note 137, 160.
[218] *Id.*, 162.
[219] *Id.*, 168.
[220] M. VAUCLAIR, préc., note 216, à la page 38.
[221] *R.* c. *Duarte*, [1990] 1 R.C.S. 30, 42-43; P. HOGG, préc., note 165, p. 48-20.3; B. MCISAAC, R. SHIELDS et K. KLEIN, préc., note 158, p. 2-44.3; M. POWER, préc., note 149, p. 250. Nous reviendrons plus longuement sur la surveillance électronique au cœur de notre réflexion, dans la partie III.

forcément invalide. Elle ne le sera que si elle ne respecte pas les exigences du paragraphe 24(2) de la *Charte canadienne*, qui prévoit que des éléments de preuve « obtenus dans des conditions qui portent atteinte aux droits ou libertés garantis par la [Charte canadienne] » seront écartés « s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice ».

Les facteurs entrant dans l'appréciation du test établi par ce paragraphe furent précisés par la Cour suprême, dans l'arrêt *R.* c. *Grant*[222]. Selon la cour, une demande d'exclusion fondée sur le paragraphe 24(2) doit permettre d'« évaluer et [de] mettre en balance l'effet que l'utilisation des éléments de preuve aurait sur la confiance de la société envers le système de justice », en tenant compte de trois éléments, à savoir « (1) la gravité de la conduite attentatoire de l'État [,] (2) l'incidence de la violation sur les droits de l'accusé garantis par la *Charte* [et] (3) l'intérêt de la société à ce que l'affaire soit jugée au fond »[223].

Au final, il s'avère que le caractère raisonnable d'une fouille, perquisition ou saisie sera évalué à la lumière d'un ensemble de principes constitutionnels ayant pour objectif de prévenir les abus étatiques, conformément à la dynamique de pondération inhérente à la conception même de l'article 8. Cette dynamique vise à assurer la prise en compte des intérêts opposés au cœur du processus de fouilles, perquisitions et saisies, au sommet desquels se trouvent la protection des droits et libertés fondamentaux, ainsi que l'application de la loi et la punition de

---

[222] *R.* c. *Grant*, [2009] 2 R.C.S. 353. La méthode d'analyse de cet arrêt quant au test du paragraphe 24(2) remplace celle précédemment énoncée dans les arrêts *R.* c. *Collins*, préc., note 213; et *R.* c. *Stillman*, préc., note 194.

[223] *R.* c. *Grant*, préc., note 222, par. 71.

la criminalité. Bref, la détermination de l'existence d'une protection constitutionnelle de la vie privée en vertu de l'article 8 sera effectuée en deux temps, tout d'abord de par l'étude du critère de l'attente raisonnable, puis ensuite à travers l'analyse du caractère raisonnable d'une fouille, perquisition ou saisie. Néanmoins, dans les situations n'impliquant pas d'actes gouvernementaux de cette nature, le niveau de vie privée dont bénéficiera un individu sera directement déterminé au niveau législatif, hors du contexte constitutionnel.

2.1.2. Les régimes législatifs de protection de la vie privée

La protection législative dont bénéficie la vie privée au Canada, tant au niveau fédéral que provincial, est considérable : plus de vingt-cinq lois visant spécifiquement la protection des renseignements personnels ont été adoptées durant les dernières décennies[224]. Ces lois établissent le cadre juridique applicable, sur une base quotidienne, à la très grande majorité des cas de figure susceptibles d'être liés à la protection de la vie privée, notamment en matière de protection des renseignements personnels. Nous ne nous intéresserons cependant pas à ces lois dans le détail, puisque leur analyse ne serait pas pertinente au développement et à l'articulation de notre réflexion. Celle-ci, de par son caractère constitutionnel et dû aux nombreuses questions fondamentalement politiques qu'elle soulève, s'effectuera en amont de la dimension législative de l'encadrement du droit à la vie privée. Ceci étant, contentons-nous de préciser que ces lois s'organisent autour de plusieurs secteurs d'intérêt bien précis et qu'à ce titre, elles peuvent être définies par les domaines auxquels elles s'appliquent : le secteur public, le secteur privé et le domaine de la santé[225].

---

[224] M. POWER, préc., note 149, p. 3.
[225] *Id.*

Tout d'abord, les lois de protection des renseignements personnels en vigueur dans le secteur public sont conçues pour prévenir la collecte, l'utilisation et la divulgation non autorisée de renseignements personnels, en plus d'accorder aux individus un droit d'accès à leurs renseignements et leur permettre d'exiger la correction de toute information inexacte détenue par les autorités publiques[226]. Le parlement canadien, les dix provinces et les trois territoires se sont dotés de lois à cet effet[227].

Les lois de protection des renseignements personnels dans le secteur privé visent quant à elles à encadrer la collecte, l'utilisation et la divulgation d'informations personnelles par les organisations dans le cadre de leurs activités commerciales[228]. Le parlement canadien et trois provinces ont adopté des lois en ce sens[229].

---

[226] *Id.*, p. 5; Michael POWER, *Access to Information and Privacy*, 1re éd., coll. « Halsbury's Law of Canada », Markham, LexisNexis, 2011, p. 194.

[227] *Privacy Act* [Canada], L.R.C. 1985, c. P-21; *Freedom of Information and Protection of Privacy Act* [Colombie-Britannique], R.S.B.C. 1996, c. 165; *Freedom of Information and Protection of Privacy Act* [Alberta], R.S.A. 2000, c. F-25; *Freedom of Information and Protection of Privacy Act* [Saskatchewan], S.S. 1990-91, c. F-22.01; *Freedom of Information and Protection of Privacy Act* [Manitoba], C.C.S.M., c. F175; *Freedom of Information and Protection of Privacy Act* [Ontario], R.S.O. 1990, c. F.31; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [Québec], L.R.Q., c. A-2.1; *Access to Information and Protection of Privacy Act* [Terre-Neuve-et-Labrador], S.N.L. 2002, c. A-1.1; *Right to Information and Protection of Privacy Act* [Nouveau-Brunswick], S.N.B. 2009, c. R-10.6; *Freedom of Information and Protection of Privacy Act* [Nouvelle-Écosse], S.N.S. 1993, c. 5; *Freedom of Information and Protection of Privacy Act* [Île-du-Prince-Édouard], R.S.P.E.I. 1988, c. F-15.01; *Access to Information and Protection of Privacy Act* [Yukon], R.S.Y. 2002, c. 1; *Access to Information and Protection of Privacy Act* [Territoires du Nord-Ouest], S.N.W.T. 1994, c. 20; et *Access to Information and Protection of Privacy Act* [Nunavut], S.N.W.T. (Nu.) 1994, c. 20.

[228] M. POWER, préc., note 149, p. 4; M. POWER, préc., note 226, p. 242.

[229] *Loi sur la protection des renseignements personnels et les documents électroniques* [Canada], L.C. 2000, c. 5; *Personal Information Protection Act* [Colombie-Britannique], S.B.C. 2003, c. 63; *Personal Information Protection Act* [Alberta], S.A. 2003, c. P-6.5; et *Loi sur la protection des renseignements personnels dans le secteur privé* [Québec], L.R.Q., c. P-39.1.

De surcroît, huit lois provinciales de protection des renseignements personnels dans le secteur de la santé sont actuellement en vigueur au pays[230]. Finalement, il existe, dans quatre provinces, un régime législatif instituant un délit civil d'atteinte à la vie privée visant à pallier les insuffisances traditionnelles de la common law en cette matière[231]. Bien qu'elles revêtent une importance capitale dans la vie quotidienne des Canadiens, il ne nous sera pas nécessaire, pour les raisons précédemment exposées, d'approfondir notre traitement de ces lois.

En conclusion, il fut démontré, dans cette sous-partie, que la part du lion de la protection dont jouit la vie privée, en droit canadien, revenait à sa dimension constitutionnelle, laquelle est fondée sur l'article 8 de la *Charte canadienne* et – bien qu'accessoirement – sur son article 7. Qu'elle soit constitutionnelle ou législative, la protection dévolue à la vie privée est considérable. Elle présente néanmoins plusieurs lacunes au regard de certains phénomènes contemporains, telle que la surveillance électronique à grande échelle des métadonnées. Cette situation justifie, à nos yeux, que nous nous penchions plus longuement sur la sphère informationnelle de la vie privée, articulée autour du concept de « Biographical core ».

---

[230] *Personal Health Information Access and Protection of Privacy Act* [Colombie-Britannique], S.B.C. 2008, c. 38; *Health Information Act* [Alberta], R.S.A. 2000, c. H-5; *Health Information Protection Act* [Saskatchewan], S.S. 1999, c. H-0.021; *Personal Health Information Act* [Manitoba], C.C.S.M., c. P33.5; *Personal Health Information Protection Act* [Ontario], S.O. 2004, c. 3, Sch. A; *Personal Health Information Act* [Terre-Neuve-et-Labrador], S.N.L. 2008, c. P-7.01; *Personal Health Information Privacy and Access Act* [Nouveau-Brunswick], S.N.B. 2009, c. P-7.05; *Personal Health Information Act* [Nouvelle-Écosse], S.N.S. 2010, c. 41.

[231] *Privacy Act* [Colombie-Britannique], R.S.B.C. 1996, c. 373; *Privacy Act* [Manitoba], R.S.M. 1987, c. P-125; *Privacy Act* [Saskatchewan], R.S.S. 1978, c. P-24; *Privacy Act* [Terre-Neuve-et-Labrador], R.S.N.L. 1990, c. P-22. Au Québec, la violation du droit à la vie privée est sanctionnée en matière civile par le régime général de responsabilité extracontractuelle du *Code civil du Québec*, L.Q. 1991, c. 64.

2.2. La vie privée informationnelle : le cadre d'analyse du « Biographical core »

Tel que mentionné précédemment et conformément au principe établi dans l'arrêt *R.* c. *Dyment*[232], l'article 8 de la *Charte canadienne* protège un éventail varié d'intérêts privés, pouvant être divisés en trois sphères, soit corporelle, territoriale et informationnelle[233]. Dans cet ordre d'idées, cette sous-partie sera consacrée exclusivement au cadre d'analyse du « Biographical core »[234], lequel conditionne la protection juridique dont jouit actuellement la vie privée informationnelle au Canada. Cette dimension de la vie privée concerne la protection dont bénéficient les individus relativement à leur identité, notamment eu égard aux renseignements intimes les concernant. Elle est particulièrement pertinente dans le contexte où des actes de l'État visent ces renseignements, notamment par le biais de fouilles, perquisitions ou saisies des communications privées. Ainsi, nous aborderons tout d'abord, dans une perspective conceptuelle, la vie privée informationnelle comme modalité d'aménagement de l'identité individuelle (2.2.1) puis, dans une perspective plus juridique, l'étendue de la protection normative de cette sphère de la vie privée (2.2.2). Nous apporterons ensuite quelques précisions sur la détermination de l'objet d'une fouille, perquisition ou saisie en matière de vie privée informationnelle (2.2.3), avant de conclure. Précisons également que les limitations du cadre d'analyse du « Biographical core » inhérentes à la surveillance électronique des métadonnées seront quant à elles traitées dans la troisième et dernière partie de ce mémoire.

---

[232] *R.* c. *Dyment*, préc., note 134, par. 19.
[233] *Supra*, 2.1.1.2.1.2.
[234] Nous avons délibérément choisi de prioriser l'expression anglaise désignant ce concept, dû au fait que l'expression « renseignements biographiques d'ordre personnel » ne nous semblait pas capter avec autant d'éloquence sa nature, voire son essence.

2.2.1. La vie privée informationnelle comme modalité d'aménagement de l'identité individuelle

Précisons, d'entrée de jeu, que la vie privée informationnelle soulève l'épineuse question des renseignements concernant les individus et leurs activités qu'il est possible de soustraire à la curiosité de l'État[235]. Cette dimension de la vie privée découle « du postulat selon lequel l'information à caractère personnel est propre à l'[individu], qui est libre de la communiquer ou de la taire comme il l'entend »[236]. La protection de l'ensemble des intérêts protégés par la vie privée est fondée sur l'autonomie morale et physique des individus[237] et, à ce titre, vise à promouvoir les valeurs sous-jacentes à l'article 8 de la *Charte canadienne* que sont la dignité, l'intégrité et l'autonomie[238]. La vie privée informationnelle est, quant à elle, fondée, au même titre que la vie privée corporelle, sur la notion de dignité et d'intégrité de la personne[239]. Bien qu'intangibles, les renseignements concernant les individus, de même que la capacité de ces individus à les contrôler, sont essentiels à ces valeurs[240]. Les valeurs que sont la dignité, l'intégrité et l'autonomie, promues par la protection du « Biographical core », peuvent donc constituer des indices nous assistant dans la détermination de l'existence d'une protection de la vie privée informationnelle et son intensité. Tous les renseignements ne se verront pas accorder la même protection, dans la mesure où ils ne promeuvent pas forcément ces valeurs,

---

[235] *R.* c. *Tessling*, préc., note 183, par. 23.
[236] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 13.
[237] *R.* c. *Dyment*, préc., note 134, par. 17.
[238] *R.* c. *Plant*, [1993] 3 R.C.S. 281, 293.
[239] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 13; *R.* c. *Dyment*, préc., note 134, par. 22.
[240] Teresa SCASSA, « Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy », (2010) 7 *Can. J. L. & Tech.* 193, 199-200.

en plus d'être susceptibles, dans certains cas, d'aller à leur encontre[241]. Ainsi, la vie privée informationnelle implique la survenance d'une violation des renseignements personnels chaque fois qu'une tierce partie en prend indûment connaissance, ce qui a pour conséquence d'amoindrir l'autonomie et de dévoiler la personnalité de l'individu concerné[242]. C'est dans cette perspective que nous appréhendons le concept de vie privée informationnelle, notamment eu égard à son potentiel quant à l'aménagement, par les individus, d'une identité propre.

Qui plus est, mentionnons, de manière complémentaire, que le droit au respect du caractère privé des renseignements personnels fut initialement défini par le professeur Westin comme étant « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués »[243]. Bien que raffinée et partiellement articulée autrement en droit canadien, cette conception de la vie privée informationnelle nous semble pertinente, ne serait-ce que pour illustrer le rôle central de l'indépendance dont jouissent les individus, dans toute société démocratique, relativement à la détermination de leur propre identité[244]. À

---

[241] Sur cette question, voir *R.* c. *Plant*, préc., note 238, 293, *R.* c. *Tessling*, préc., note 183; et C. MICHAELSON, préc., note 193, 93-94 et 102. À ce sujet, Michaelson écrit, à la page 102 de son article : « not all information promotes dignity, integrity and autonomy. Indeed, some information, such as information relating to criminal acts, undermines these values. The man who beats his spouse, the purveyor of child pornography, the drug trafficker who manufactures and distributes methamphetamine, none of these can legitimately claim that information concerning their conduct should remain private to promote their dignity, integrity and autonomy. In many instances, however, they may be able to shelter such information behind other proper privacy claims. Although the spouse beater may have no legitimate privacy claim in relation to the fact that he beats his spouse, he can nonetheless shelter himself behind his general right to privacy in his home ».

[242] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 14.

[243] *R.* c. *Tessling*, préc., note 183, par. 23. Pour plus de détails, voir A. F. WESTIN, préc., note 1, p. 7.

[244] Le traitement judiciaire canadien a permis d'identifier deux conceptions principales de la vie privée, soit le droit de ne pas être importuné et le droit de contrôler l'accès à ses informations personnelles. La première conception fut initialement élaborée par la Cour suprême américaine dans l'arrêt *Katz* v. *United States*, préc., note 164, 350, puis reprise par la Cour suprême du Canada, dans l'arrêt *Hunter* c. *Southam Inc.*, préc., note

ce titre, la protection de la vie privée informationnelle concerne, en droit canadien, les renseignements touchant aux « aspects de l'identité personnelle que le droit […] vise à protéger de l'influence envahissante de l'État »[245]. L'importance fondamentale que revêt la vie privée informationnelle dans la vie des individus, leur bien-être et la détermination de leur identité justifie que lui soit accordée une protection juridique conséquente. Nous nous pencherons désormais sur l'étendue de cette protection en droit canadien.

2.2.2. La protection normative de la vie privée informationnelle

Certains auteurs soutiennent que la protection accordée aux renseignements relatifs à l'identité d'un individu serait aussi importante que celle dévolue à la vie privée corporelle, laquelle est considérable[246]. Or, le processus visant à déterminer de l'existence et de la portée d'une protection constitutionnelle de la vie privée n'est pas, comme nous le verrons, aussi simple et direct dans la sphère informationnelle qu'il l'est dans la sphère corporelle. Dans cette optique, la vie privée est un concept malléable dont l'appréhension peut s'avérer excessivement complexe, particulièrement en ce qui a trait à la limite entre ce qui relève du domaine public versus ce qui échoit à la sphère privée[247]. Comme le soulignait le juge Binnie dans l'arrêt *Tessling*, le caractère protéiforme de la vie privée rend difficile la fixation de la

---

137, 159-160. La seconde conception fut élaborée ou, du moins, définie par Alan Westin. Voir A. F. WESTIN, préc., note 1, p. 7. Nous ne nous intéresserons qu'à cette dernière conception, dans la mesure où elle nous semble plus pertinente eu égard à la vie privée informationnelle. Pour plus de détails, voir Erin MORGAN, « Surveillance and Privacy in the 21st Century : The Impact of Bills C-51 (*IP21C*) and C-52 (*IPCEC*) », (2010) 43 *U.B.C. L. Rev.* 471, 482.

[245] *Thomson Newspapers Ltd.* c. *Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425, 518.

[246] S. BOUCHER et K. LANDA, préc., note 163, p. 60.

[247] C. MICHAELSON, préc., note 193, 90-91.

limite du « caractère raisonnable » de l'expectative de protection de ce droit[248]. La solution à cette difficulté réside, en ce qui a trait à la dimension informationnelle de la vie privée, dans les enseignements de la Cour suprême du Canada relatifs à la portée de l'article 8 de la *Charte canadienne*, tout d'abord dans l'arrêt *R.* c. *Plant*[249], puis dans la jurisprudence constitutionnelle subséquente articulée autour des principes y ayant été développés. La cour, se fondant sur les principes établis dans l'arrêt *Dyment*, s'est fortement inspirée de l'arrêt de la Cour suprême américaine dans l'affaire *United States* v. *Miller*[250], dans lequel il fut déterminé que la protection constitutionnelle dont jouit la vie privée informationnelle en droit américain, en vertu du quatrième amendement, est limitée aux informations de nature « personnelle et confidentielle ». Ainsi, la Cour suprême du Canada a développé, dans l'arrêt *Plant*, le cadre d'analyse du « Biographical Core ». En raison de son importance fondamentale, nous croyons qu'il est nécessaire de reproduire intégralement le passage où la cour en expose la portée :

> Étant donné les valeurs sous-jacentes de dignité, d'intégrité et d'autonomie qu'il consacre, il est normal que l'art. 8 de la *Charte* protège un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État. Il pourrait notamment s'agir de renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu.[251] (nos soulignements)

Sont donc constitutionnellement protégés, en droit canadien, les renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État. L'emploi du terme « notamment » dans cet extrait signifie néanmoins que la vie privée informationnelle protège

---

[248] *R.* c. *Tessling*, préc., note 183, par. 25.
[249] *R.* c. *Plant*, préc., note 238.
[250] *United States* v. *Miller*, [1976] 425 US 435.
[251] *R.* c. *Plant*, préc., note 238, 293.

un éventail de renseignements plus large que les seuls renseignements « tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu »[252]. Toujours dans l'arrêt *Plant*, la Cour a ciblé, conformément à l'analyse de l'ensemble des circonstances établie dans l'arrêt *Edwards*[253], certains éléments pouvant nous aider à déterminer si un individu bénéficie d'une attente raisonnable de vie privée à l'égard de renseignements précis, à savoir « [leur] nature […], celle des relations entre la partie divulguant les renseignements et la partie en réclamant la confidentialité, l'endroit où ils ont été recueillis, les conditions dans lesquelles ils ont été obtenus et la gravité du crime faisant l'objet de l'enquête »[254]. La cour a jugé, dans un arrêt plus récent, que la portée de la protection constitutionnelle du droit de l'individu de soustraire des renseignements personnels à la connaissance de l'État dépendait de leur nature et du but dans lequel ils étaient communiqués[255]. La nature des renseignements est d'ailleurs un élément critique dans le cadre de l'analyse de l'expectative raisonnable de vie privée[256].

Par conséquent, plus un renseignement est intime, plus il est raisonnable de s'attendre à ce qu'il bénéficie d'une protection importante[257]. Il fut établi que les préoccupations en matière de vie privée relatives à « la liberté ou [au] droit de ne pas être importuné par l'État

---

[252] *R.* c. *Tessling*, préc., note 183, par. 25-26.
[253] *R.* c. *Edwards*, préc., note 174.
[254] *R.* c. *Plant*, préc., note 238, 293.
[255] *R.* c. *Gomboc*, [2010] 3 R.C.S. 211, par. 27.
[256] W. N. RENKE, préc., note 84, 803; et Richard JOCHELSON, « Trashcans and Constitutional Custodians : The Liminal Spaces of Privacy in the Wake of Patrick », (2009) 72 *Sask. L. Rev.* 199, 204.
[257] Michael POWER, *Halsbury's Law of Canada. Access to Information and Privacy*, Markham, LexisNexis, 2011, p. 416. Power avance également, suivant les enseignements de l'arrêt *R.* c. *Plant*, préc., note 238, que « [f]or information to be granted protection under s. 8, it should contain the following characteristics: be of a personal and confidential nature; affect and relate to a biographical core of personal information; and reveal intimate details of the lifestyle and personal choices of the individual ». Voir également Janis L. GOLDIE, « Virtual Communities and the Social Dimension of Privacy », (2006) 3-1 *R.D.T.U.O.* 133, par. 7.

»[258] sont « à leur plus fort lorsque des aspects de l'identité d'une personne sont en jeu, comme dans le cas des renseignements ‘’relatifs [à son mode de vie], à ses relations intimes ou à ses convictions politiques ou religieuses’’ »[259]. Ceci étant, un auteur soutient que les renseignements suivants seraient visés par le « Biographical core » : les opinions et affiliations politiques ou religieuses, le statut financier et professionnel, l'orientation et les pratiques sexuelles, les relations personnelles et les préférences romantiques, l'état de santé et l'hygiène personnelle, les pensées, de même que des activités aussi anodines que le fait de prendre un bain ou d'allumer les lumières à un moment inhabituel du jour ou de la nuit[260].

De surcroît, la Cour suprême a récemment reconnu, dans l'arrêt *R.* c. *Spencer*, que la vie privée informationnelle englobait trois facettes conceptuellement distinctes, mais appelées à se chevaucher, soit la confidentialité, le contrôle et l'anonymat[261]. La confidentialité concerne le respect du caractère privé des renseignements individuels[262], alors que le contrôle porte sur la gestion de l'accès à l'information et sur l'utilisation des renseignements par autrui[263]. L'anonymat va encore plus loin et concerne, quant à lui, la protection de la confidentialité de l'identité[264]. Ces trois facettes sont autant d'éléments spécifiques pouvant nous aider à

---

[258] *R.* c. *Mills*, [1999] 3 R.C.S. 668, par. 79.
[259] *Id.*, par. 80.
[260] Alexandre GENEST, « Privacy as Construed During the Tessling Era: Revisiting the "Totality of Circumstances Test", Standing and Third Party Rights », (2007) 41 *R.J.T.* 337, 375.
[261] *R.* c. *Spencer*, préc., note 186, par. 38.
[262] *Id.*, par. 39.
[263] *Id.*, par. 40; Voir également *R.* c. *Dyment*, préc., note 134, où la cour énonce, aux pages 429-430 : « [d]ans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués ».
[264] *R.* c. *Spencer*, préc., note 186, par. 42-44. Voir également A. F. WESTIN, préc., note 1, p. 31-32.

déterminer, dans une situation donnée, l'existence d'une protection de la vie privée informationnelle.

Dans une perspective plus concrète, la Cour suprême a précisé, dans l'arrêt *R.* c. *Cole*, que plus l'objet d'une fouille, perquisition ou saisie se trouve près de l'ensemble des renseignements biographiques d'ordre personnel, plus l'existence d'une attente raisonnable en matière de respect de la vie privée en sera favorisée[265]. Il en découle que plus des renseignements seront personnels et confidentiels, plus des individus raisonnables et bien informés seront disposés à reconnaître que la Constitution garantit l'existence d'un droit au respect de la vie privée informationnelle[266].

Finalement, il est bien établi, dans la jurisprudence constitutionnelle, que la catégorisation des renseignements, notamment comme étant des « renseignements biographiques d'ordre personnel »[267] constitue un moyen d'analyse et non une classification stricte[268]. Il importe également de préciser que le fait de savoir si des renseignements relèvent du « Biographical core » et, incidemment, s'ils bénéficient de la protection du droit à la vie privée informationnelle, sera déterminé au cas par cas, par les tribunaux, en fonction de

---

[265] *R.* c. *Cole*, [2012] 3 R.C.S. 34, par. 46.
[266] *Id.*
[267] *R.* c. *Plant*, préc., note 238, 293.
[268] Voir l'arrêt *R.* c. *A.M.*, [2008] 1 R.C.S. 569, dans lequel la Cour suprême écrit, au paragraphe 68: « [d]ans *Dyment*, *Plant* et *Tessling*, les diverses catégories de ''renseignements'' (y compris les ''renseignements biographiques d'ordre personnel'') ont servi de moyen d'analyse utile et non de moyen de classification qui doit être déterminant pour l'analyse du droit à la vie privée sur les renseignements personnels. Ce ne sont pas tous les renseignements ne satisfaisant pas au critère des « renseignements biographiques d'ordre personnel » qui sont accessibles à la police ».

l'analyse de l'ensemble des circonstances d'une situation donnée[269]. Bref, les individus ne jouissent, en droit canadien, d'aucun « droit général à la vie privée » relativement à leurs informations personnelles, mais plutôt seulement d'un droit à la protection de leurs « renseignements biographiques d'ordre personnel »[270]. Ceux-ci sont tout de même en droit de s'attendre à un niveau minimal de protection de leur vie privée, sans égard à la nature spécifique de l'atteinte étatique, donc à la méthode de surveillance utilisée[271]. Nous analyserons désormais, à des fins de précision et dans une optique complémentaire, la question plus procédurale de la détermination de l'objet d'une fouille, perquisition ou saisie en matière de vie privée informationnelle.

2.2.3. La détermination de l'objet d'une fouille, perquisition ou saisie en matière de vie privée informationnelle

Il nous apparaît essentiel, avant d'être en mesure de réfléchir à la protection de la vie privée informationnelle au regard de la collecte et de la surveillance à grande échelle des métadonnées[272], d'insister sur un élément fondamental du processus d'analyse que commande l'article 8 de la *Charte canadienne*. Ainsi, nous traiterons des particularités inhérentes à la détermination de l'objet d'une fouille, d'une perquisition ou d'une saisie en matière de vie privée informationnelle. La pertinence de traiter ici de cet élément réside dans le fait que la

---

[269] Voir les arrêts *R.* c. *Edwards*, préc., note 174, par. 45, dans lequel la Cour suprême a établi le principe de la totalité des circonstances, puis *R.* c. *Tessling*, préc., note 183, par. 31-32, concernant l'adaptation de ce principe en matière de vie privée informationnelle.
[270] M. POWER, préc., note 149, p. 237.
[271] S. PENNEY, préc., note 163, 112.
[272] *Infra*, partie III.

protection normative dont bénéficie cette dimension de la vie privée est intimement liée à la détermination appropriée de l'objet d'une fouille, perquisition ou saisie.

Les tribunaux canadiens ont eu, par le passé, l'opportunité de se prononcer sur la protection de la vie privée informationnelle dans le cadre d'un éventail relativement varié de situations. Ce processus présente parfois une certaine ambiguïté, particulièrement lorsque des intérêts inhérents à la vie privée informationnelle sont touchés par les actions de l'État. Une telle ambiguïté est d'ailleurs propre à cette dimension de la vie privée. Nous n'aurions donc aucune difficulté à concevoir et à appréhender la nature des droits en matière de vie privée auxquels les actes de l'État seraient susceptibles de porter atteinte lorsque, par exemple, un policier effectue une fouille corporelle agressive d'un prévenu ou encore s'il fait irruption dans une résidence privée pour y chercher des preuves. Sans pour autant nous prononcer sur l'ensemble des principes entourant la légalité de tels actes, il nous apparaît évident, dans le premier cas, que les agissements de l'État sont potentiellement attentatoires aux intérêts corporels protégés par le droit à la vie privée, alors qu'ils le sont aux intérêts territoriaux dans le second. Le cas de la vie privée informationnelle s'avère toutefois beaucoup plus délicat, ne serait-ce que dû à la nature intangible des renseignements et à leur complexité.

Les autorités étatiques allèguent parfois, dans l'optique de restreindre l'expectative de vie privée d'un accusé, avoir surveillé et saisi « uniquement » des renseignements d'un certain type, tels qu'un nom, une adresse, ou un numéro de téléphone. Or, une telle position ne serait pas envisageable dans le cas d'une fouille corporelle ou d'une perquisition dans une maison d'habitation. Il serait ainsi inconcevable que l'État prétende n'avoir « que vérifié le contenu de

la poche » d'un prévenu ou encore « simplement enfoncé la porte d'une maison d'habitation pour y recueillir un objet quelconque ». Il s'agirait plus exactement – et sans aucun doute – d'une fouille corporelle et d'une fouille dans une résidence privée.

Quelques précisions sur l'interprétation et l'application de l'article 8 s'imposent pour clarifier l'ambiguïté que présente le cas de la vie privée informationnelle en cette matière[273]. Tout d'abord, la jurisprudence constitutionnelle a clairement établi que si « l'activité de [l'État] a pour effet de déjouer une attente raisonnable en matière de respect de la vie privée », elle constituera une fouille[274]. Il en découle que les fouilles, perquisitions et saisies seront appréhendées relativement aux conséquences qu'elles sont susceptibles d'entraîner sur les individus visés[275]. Il ne faut donc pas se restreindre aux actions commises par l'État ou à l'espace envahi, mais plutôt se concentrer sur « la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte »[276]. L'arrêt *R.* v. *Trapp*[277], de la Cour d'appel de la Saskatchewan, est très illustratif à cet effet.

Dans cette affaire, les autorités policières avaient obtenu, après avoir procédé à la surveillance de fichiers en ligne contenant de la pornographie juvénile, des renseignements

---

[273] Nous traiterons toutefois plus en profondeur des principes d'interprétation constitutionnelle dans la partie III de ce mémoire.

[274] *R.* c. *Wise*, préc., note 175, 533.

[275] *R.* c. *Evans*, [1996] 1 R.C.S. 8. Selon la cour, ce n'est « que lorsque les enquêtes de l'État empiètent sur un droit raisonnable des particuliers à la vie privée que l'action gouvernementale en cause constitue une ''fouille ou perquisition'' au sens de l'art. 8 » (par. 11). Voir également *R.* c. *Buhay*, [2003] 1 R.C.S. 631, par. 33-34; *R.* c. *Law*, [2002] 1 R.C.S. 227, par. 15; *R.* c. *Tessling*, préc., note 183, par. 18; et *R.* c. *Gomboc*, préc., note 255, par. 77.

[276] *R.* c. *Spencer*, préc., note 186, par. 31, citant avec approbation le paragraphe 65 de l'arrêt de la Cour d'appel de l'Ontario dans l'affaire *R.* v. *Ward*, [2012] ONCA 660.

[277] *R.* v. *Trapp*, [2011] SKCA 143. Le raisonnement de la Cour d'appel à cet égard fut confirmé par la Cour suprême dans l'arrêt *R.* c. *Spencer*, préc., note 186, par. 26.

d'identification concernant l'adresse IP de M. Trapp auprès de son fournisseur d'accès Internet. Ces renseignements comprenaient des informations sur son dossier de client auprès dudit fournisseur, incluant son nom, son adresse et son numéro de téléphone[278] et ont, par la suite, permis aux autorités policières d'obtenir un mandat autorisant la perquisition de son domicile[279]. Lors du procès, le juge a rejeté l'argument de l'accusé selon lequel le mandat de perquisition aurait été lancé sur le fondement d'informations obtenues illégalement, en contravention de l'article 8 de la *Charte canadienne*, et celui-ci fut reconnu coupable des infractions reprochées[280]. En appel, dans le cadre du débat sur l'objet de la fouille ayant mené à l'obtention des informations d'identification de M. Trapp et, conséquemment, sur l'expectative de vie privée dont ce dernier bénéficiait à leur égard, les procureurs de la Couronne ont tenté de minimiser le caractère sensible desdites informations :

> We heard a good deal of argument about this, replete with all manner of analogy. Leaving aside the analogies, which are only distracting, counsel for the Attorney General contended that the information in question does not contain a biographical core of personal information, for it is merely "subscriber information" or "customer information." Or it is nothing more than "name, address, and telephone number information" published in the telephone directory and available in the public domain; or "tombstone-like" information.[281] (nos soulignements)

La cour a toutefois jugé qu'il importait d'aller au-delà d'un exercice sommaire de caractérisation, voire d'étiquetage, des renseignements en question et que la simple caractérisation du type de renseignement n'est pas, en pareilles circonstances, particulièrement utile, en plus d'être susceptible de fausser le processus d'analyse :

> With respect I do not find these characterizations to be particularly helpful. The information that forms the subject matter of the alleged search is what it is. And it

[278] *R.* v. *Trapp*, préc., note 277, par. 75-79.
[279] *Id.*, par. 81.
[280] *Id.*, par. 83-84.
[281] *Id.*, par. 34.

> seems to me there is no need to label it. Either it contains a biographical core of personal information or it does not, and I think it is unhelpful to the determination of that issue to label the information in some such way. Even worse, such labels are apt to skew the analysis. To label information of this kind as mere "subscriber information" or "customer information", or nothing but "name, address, and telephone number information", tends to obscure its true nature.[282] (nos soulignements)

Ainsi, plutôt que de concevoir, par exemple, des renseignements comme n'étant que des « informations sur le dossier du client » ou encore « un nom, une adresse ou un numéro de téléphone »[283], il importe de se concentrer sur leur *qualité* intrinsèque, à savoir leur potentiel quant à la révélation d'informations sur l'individu et ses activités[284]. La seule question pertinente est donc celle de savoir si les renseignements analysés présentent un « caractère biographique d'ordre personnel »[285] et, à ce titre, sont visés par le « Biographical core »[286]. Qui plus est, la Cour suprême a récemment précisé qu'il est crucial, en matière de vie privée informationnelle, de « tenir compte de la tendance qui consiste à chercher à obtenir des renseignements pour permettre d'en tirer des inférences au sujet d'autres renseignements qui, eux, sont de nature personnelle »[287]. Ce point sera crucial dans notre analyse du cas des métadonnées.

Bref, il sera nécessaire, dans le cadre de la détermination de l'objet d'une fouille, perquisition ou saisie et, par extension, de l'expectative de vie privée en matière informationnelle, de se garder de procéder par le biais d'une approche trop axée sur le type de renseignement analysé. Une telle approche pourrait nous inciter, à tort, à « étiqueter » lesdits

---

[282] *Id.*, par. 35.
[283] *Id.*
[284] *Id.*, par. 37.
[285] *Id.*, par. 35.
[286] *R.* c. *Plant*, préc., note 238, 293.
[287] *R.* c. *Spencer*, préc., note 186, par. 31.

renseignements, au détriment de leur caractère réel et de l'impact que les actes de l'État sont susceptibles d'avoir sur l'attente qu'entretiennent les individus à l'égard de leur vie privée informationnelle.

En conclusion, cette sous-partie nous a permis de noter que le cadre d'analyse du « Biographical core » est devenu, durant les deux décennies ayant suivi son élaboration, un élément central de la jurisprudence constitutionnelle entourant le droit à la vie privée[288]. Il consacre l'importance de l'aménagement d'une sphère d'autonomie individuelle et de protection de l'identité de tout un chacun, en garantissant aux individus un certain contrôle sur les renseignements les plus intimes les concernant. Ce faisant, il permet à ces individus, en toute indépendance, de façonner et de déterminer leur identité propre, hors de la contrainte et de l'influence des agents de l'État[289]. Le « Biographical core » vise spécifiquement la protection des individus contre cette influence, par le biais de l'établissement d'un cadre d'analyse propre à assurer, concrètement, l'aménagement d'une sphère de renseignements intimes protégée contre toute atteinte injustifiée de l'État. Cette approche est conforme aux objectifs centraux que sont, au sein de toute démocratie libérale, la préservation de la dignité et l'intégrité de la personne.

Ceci étant, le cadre d'analyse du « Biographical core » protège les renseignements biographiques qu'il serait raisonnable pour les individus de vouloir soustraire à la connaissance de l'État, dans la mesure où ceux-ci pourraient potentiellement révéler des

---

[288] Alysia DAVIES, « Invading the Mind : The Right to Privacy and the Definition of Terrorism in Canada », (2006) 3-1 *R.D.T.U.O.* 249, 270.

[289] L'importance de processus est, comme nous la vu dans la première partie ce mémoire, fondamentale.

détails intimes sur les choix et les activités de ces individus. La vie privée informationnelle concerne donc, à travers ses trois facettes que sont la confidentialité, le contrôle et l'anonymat, les renseignements qui sont les plus fondamentaux dans nos vies individuelles. De plus, il nous est possible d'affirmer que plus un renseignement présente un caractère intime, plus il est susceptible de se voir accorder une protection juridique importante par les tribunaux. Si la vie privée informationnelle jouit, en soi, d'une importante protection, elle constitue également un élément dont il sera nécessaire, sur le plan procédural, de tenir compte, particulièrement à l'étape de la détermination de l'objet d'une fouille, perquisition ou saisie contestée. Conséquemment, il sera crucial de se concentrer sur la qualité intrinsèque des renseignements visés, au détriment de leur type ou de tout autre exercice de catégorisation susceptible d'en fausser l'analyse. Il importe, par ailleurs, de garder à l'esprit que la détermination du caractère biographique et personnel des renseignements protégés par le cadre d'analyse du « Biographical core », participe du processus global, dans une situation donnée, de pondération de l'ensemble des circonstances pertinentes.

Conclusion provisoire

Cette deuxième partie du mémoire avait comme objectif de présenter l'étendue de la protection normative dévolue, en droit constitutionnel canadien, au droit à la vie privée. Cet exercice nous a permis de présenter les principes fondamentaux conditionnant l'articulation de cette protection constitutionnelle, de même que ses limitations. Ainsi, nous avons démontré, dans une première sous-partie, que la protection accordée au droit à la vie privée est, en droit canadien, considérable. Pour ce faire, nous avons concentré notre analyse sur les articles 7 et 8 de la *Charte canadienne*. D'une part, l'article 7 de la *Charte canadienne* prévoit une

protection limitée du droit à la vie privée, ne serait-ce qu'indirectement et partiellement, par le biais de l'interprétation jurisprudentielle de la portée des droits à la liberté et à la sécurité. Il en va, dans ces deux cas, du caractère fondamental de certaines décisions que peut prendre tout individu sur son existence et son intégrité. D'autre part, il ressort de notre étude que l'essentiel de la protection constitutionnelle découle du droit à la protection contre les fouilles, perquisitions ou saisies abusives, prévu à l'article 8 de la *Charte canadienne*. C'est d'ailleurs cette disposition qui établit le cadre méthodologique propre à l'analyse juridique de toute atteinte directe au droit à la vie privée résultant d'une action gouvernementale au Canada. Sans pour autant revenir en détail sur le raisonnement propre à appréhender de telles violations, rappelons toutefois qu'il s'articule autour de la notion d'attente raisonnable en matière de vie privée et de son intensité, en fonction d'un ensemble de circonstances, notamment du type d'intérêt privé en question.

Nous nous sommes ensuite intéressés, plus spécifiquement, à la vie privée informationnelle. Cette dimension de la vie privée s'appréhende conformément au cadre d'analyse du « Biographical core », en vertu duquel seuls les renseignements présentant un caractère biographique d'ordre personnel et susceptibles de révéler des détails intimes sur les choix et le mode de vie d'un individu sont protégés. Or, nous sommes forcés de constater que le concept de vie privée informationnelle présente, à sa face même, plusieurs difficultés en complexifiant l'étude. L'intangibilité et la nature intrinsèquement diffuse des renseignements rendent plus ardue la détermination précise de l'objet d'une fouille, perquisition ou saisie en matière informationnelle, de même que l'existence et le niveau approprié d'une quelconque protection constitutionnelle. Il en résulte une incertitude quant à la capacité du « Biographical

core » d'assurer à la vie privée informationnelle une protection constitutionnelle réellement effective.

Il est admis que la démarche de pondération au cœur même du régime des droits et libertés fondamentaux présuppose, dans plusieurs situations, une certaine limitation du droit à la vie privée. Ainsi, la protection législative d'un ensemble d'intérêts tantôt convergents, tantôt divergents implique, voire nécessite parfois une réduction corrélative de la protection accordée à la vie privée[290]. Il existe cependant un seuil en dessous duquel la diminution de cette protection rendrait bien illusoire l'exercice du droit à la vie privée, particulièrement dans le contexte de la surveillance[291]. Toute inadéquation entre l'intensité de la protection du droit à la vie privée et son importance fondamentale[292] rend bien réel le spectre que soulèvent la surveillance électronique gouvernementale et la collecte à grande échelle des métadonnées[293] eu égard à la place qu'occupent, au sein de la démocratie canadienne, les droits et libertés fondamentaux, à commencer par la vie privée. Nous sommes toutefois pleinement conscients des risques qu'implique toute conclusion hâtive à cet égard. Nous sommes également conscients du fait que la gravité de la menace terroriste planétaire commande une réflexion posée et rationnelle sur les enjeux de la surveillance gouvernementale à des fins de sécurité

---

[290] Nous n'aurions, par exemple, qu'à penser à la liberté d'expression, à la recherche scientifique ou encore à l'application de la loi. Voir R. GAVISON, préc., note 29, 457-458.

[291] À propos de la surveillance électronique, le juge La Forest écrivait, dans l'arrêt *R.* c. *Duarte*, préc., note 221, 44, que « si l'État était libre de faire, à son entière discrétion, des enregistrements électroniques permanents de nos communications privées, il ne nous resterait rien qui vaille de notre droit de vivre libre de toute surveillance. La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications restent privées. Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens ». Voir également *R.* c. *Wong*, préc., note 178, 47.

[292] *Supra*, sous-partie 1.1.

[293] *Supra*, sous-partie 1.2.

nationale et de la protection du droit à la vie privée. Il est donc essentiel de se garder d'adopter, à leur égard, une position trop tranchée.

Bref, c'est dans cette optique que nous confronterons le cadre d'analyse du « Biographical core » au concept de métadonnée, dans la troisième partie de ce mémoire. Nous espérons, par la suite, être en mesure de nous prononcer avec plus de certitude sur la capacité effective du « Biographical core » à protéger aujourd'hui le droit à la vie privée informationnelle.

3. VERS UNE NOUVELLE CONCEPTION DE LA VIE PRIVÉE?

> *As every man goes through life he fills a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread, permanently connecting him to the local centre of personnel records administration. There are thus hundreds of little threads radiating from every man, millions of threads in all.* […] *They are not visible, they are not material, but every man is constantly aware of their existence. The point is that a so-called completely clean record was almost unattainable, an ideal, like absolute truth. Something negative of suspicious can always be noted down against any man alive. Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find out what it is.*
>
> Aleksandr Solzhenitsyn[294]

Introduction

Le cœur de notre réflexion est présenté sous forme d'un argumentaire juridique essentiellement fondé sur la définition juridique du droit à la vie privée au Canada, plus particulièrement sur la portée constitutionnelle de la garantie contre les fouilles, perquisitions et saisies abusives prévue à l'article 8 de la *Charte canadienne*. Dans cet ordre d'idées, nous avons tout d'abord traité, dans la première partie de ce mémoire, de l'importance et du caractère fondamental de la vie privée dans l'existence des individus et leur épanouissement[295], mais aussi de l'aménagement et de la protection des processus sociaux inhérents à notre conception canadienne d'une démocratie libérale[296]. Nous avons également pu constater, toujours dans cette première partie, que les métadonnées des communications électroniques étaient susceptibles de révéler des informations intimes potentiellement

---

[294] Aleksandr SOLZHENITSYN, *Cancer Ward*, Londres, Vintage, 2003, p. 208.
[295] *Supra*, 1.1.1.
[296] *Supra*, 1.1.2.

privées[297]. Ceci étant, nous y avons analysé la nature et l'étendue des activités gouvernementales de surveillance électronique et de collecte à grande échelle de ces métadonnées et il nous est aussitôt apparu nécessaire qu'elles bénéficient d'une protection juridique appropriée[298].

Dans ce contexte, nous nous sommes intéressés, dans la deuxième partie de ce mémoire, à la teneur de la protection constitutionnelle de la vie privée en droit canadien, à travers l'étude des articles 7 et 8 de la *Charte canadienne*[299] puis, plus spécifiquement, des principes juridiques conditionnant la protection de la vie privée informationnelle[300]. Nous sommes toutefois forcés de constater, à cette étape de notre raisonnement, que la question de la nature de la protection juridique des métadonnées des communications électroniques demeure, à ce jour, en suspens, particulièrement à la lumière des potentielles dérives que risquent d'induire certaines activités contemporaines de surveillance électronique à grande échelle menées au nom de la sécurité nationale.

Le spectre que font surgir ces activités pour la démocratie canadienne, si elles n'étaient pas adéquatement circonscrites, nous contraint donc, dans la troisième et dernière partie de ce mémoire, à nous interroger sur la teneur de la garantie contre les fouilles, perquisitions et saisies abusives prévue à l'article 8 de la *Charte canadienne*. Essentiellement, nous argumenterons en faveur d'un élargissement de la portée du cadre d'analyse constitutionnel

---

[297] *Supra*, 1.2.1.
[298] *Supra*, 1.2.2.
[299] *Supra*, 2.1.
[300] *Supra*, 2.2.

actuel de la vie privée informationnelle, à savoir le « Biographical core », dans l'optique de protéger adéquatement les métadonnées des communications électroniques face à certaines pratiques gouvernementales visant leur surveillance électronique et leur collecte à grande échelle. Pour ce faire, nous nous pencherons tout d'abord sur la question de la protection juridique qu'est susceptible de conférer le « Biographical core » aux métadonnées des communications électroniques (3.1), ainsi qu'au contexte social global dans lequel s'insère notre réflexion (3.2). Advenant le cas où le « Biographical core » ne nous semblerait pas en mesure d'y parvenir, nous serions contraints de conclure qu'une nouvelle conception du droit à la vie privée informationnelle s'avèrerait nécessaire afin d'assurer une pleine protection aux métadonnées des communications électroniques.

3.1. La protection juridique des métadonnées des communications électroniques

Nous constatons, d'entrée de jeu, que la question de la protection juridique des métadonnées des communications électroniques n'a pas, à ce jour, été tranchée par les tribunaux canadiens[301]. La Cour suprême du Canada a toutefois expressément mentionné, en 2008, dans l'arrêt *R.* c. *A.M*, qu'en raison de l'évolution rapide caractérisant le domaine de la vie privée et de la protection des renseignements personnels, il est essentiel, « afin de tracer la limite de ce qui est raisonnable » de « revenir encore et encore aux principes fondamentaux »[302]. Ce faisant, nous estimons que l'élaboration d'une protection plus adéquate des métadonnées des communications électroniques nécessite, face à la surveillance

[301] Néanmoins, voir E. MORGAN, préc., note 244, où l'auteure se penche brièvement sur la question de l'existence, dans le contexte de la téléphonie cellulaire, d'une protection constitutionnelle des informations concernant le dossier du client (p. 484 et s.) ou les données de transmission et de localisation (p. 490 et s.). Voir également, plus généralement B. MCISAAC, R. SHIELDS et K. KLEIN, préc., note 158, p. 2-44.7 à 2-48.1.

[302] *R.* c. *A.M.*, préc., note 268, par. 39.

gouvernementale, que nous centrions notre argumentaire autour du concept fondamental qu'est le « Biographical core ». Ainsi, nous conserverons ce cadre d'analyse comme cœur opérationnel du raisonnement propre à la détermination, en droit canadien, du caractère privé d'un renseignement, et en proposerons un élargissement de la portée, de manière à inclure, tel que nous le démontrerons, les métadonnées des communications électroniques. Or, dans la mesure où la tendance actuelle, caractérisée par une démocratisation du recours aux nouvelles technologies de l'information et des communications, ainsi que leur raffinement, implique qu'une quantité toujours croissante de métadonnées soient générées, il nous apparaît essentiel, voire logique, que la portée du cadre d'analyse du « Biographical core » soit élargie afin d'inclure celles-ci. Dans cet ordre d'idées, il sera, tout d'abord, démontré que ces métadonnées constituent indéniablement, sur les plans juridique et conceptuel, des « renseignements biographiques d'ordre personnel » (3.1.1), avant d'exposer en quoi un élargissement de la portée du « Biographical core » est conforme aux principes consacrés d'interprétation de l'article 8 de la *Charte canadienne* (3.1.2).

3.1.1. Les métadonnées des communications électroniques comme renseignements biographiques d'ordre personnel

Les renseignements individuels qu'il est possible d'obtenir grâce à la surveillance électronique à grande échelle et à la collecte des métadonnées des communications électroniques sont directement visés par l'essence même de ce que vise à protéger le « Biographical core ». Ce cadre d'analyse, rappelons-le, conditionne la protection juridique dont

jouit la vie privée informationnelle en droit canadien[303]. À ce titre, il prévoit, conformément aux enseignements de l'arrêt *R.* c. *Plant*, que seront constitutionnellement protégés uniquement les « renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État »[304]. Il pourrait, selon la Cour suprême, « notamment s'agir de renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu »[305]. Conséquemment, nous considérons que l'ensemble des facteurs pertinents est favorable, au regard du contexte contemporain, à ce que la portée du « Biographical core » soit élargie, afin de permettre aux métadonnées des communications électroniques de bénéficier de cette protection constitutionnelle. Afin de le démontrer, nous nous pencherons, dans un premier temps, sur l'agrégation de ces métadonnées (3.1.1.1), avant de traiter de la désuétude, dans le contexte strictement juridique, de la distinction contenu-métadonnées (3.1.1.2), puis d'analyser la question de la qualité intrinsèque des renseignements visés par la surveillance électronique gouvernementale à grande échelle (3.1.1.3).

3.1.1.1. L'agrégation et l'analyse des métadonnées, ou le caractère fondamentalement invasif de la surveillance gouvernementale

Précisons, tout d'abord, que le simple fait que des informations spécifiques ne présentent pas, à leur face même, de caractère biographique d'ordre personnel, ne saurait justifier qu'elles ne bénéficient d'aucune protection en vertu de l'article 8 de la *Charte canadienne*. Alors que

---

[303] *Supra*, 2.2.
[304] *R.* c. *Plant*, préc., note 238, 293.
[305] *Id.*

des auteurs se sont déjà intéressés, dans cette optique, à l'enregistrement ciblé des numéros de téléphone[306] et à la surveillance vidéo[307], notre position, en ce qui a trait aux métadonnées, se fonde sur la nature même de celles-ci, ainsi que sur la teneur des activités gouvernementales de surveillance déployées à leur égard, à savoir l'analyse informatisée d'ensembles de métadonnées agrégées. Un tel procédé rend, à nos yeux, ces pratiques de surveillance particulièrement attentatoires pour la vie privée. Ceci étant, nous reconnaissons que les métadonnées générées par les communications électroniques ne présentent pas toutes, prises individuellement et hors de leur contexte, le même caractère intime que le contenu desdites communications[308]. Malgré le fait que certaines métadonnées soient susceptibles, à leur face même, de communiquer des renseignements de nature privée[309], ce n'est qu'une fois agrégées qu'elles deviennent potentiellement extrêmement révélatrices, notamment en ce qui a trait aux renseignements biographiques d'ordre personnel. Qui plus est, la nature privée des

---

[306] Wayne N. Renke avance que la procédure d'obtention d'une autorisation préalable à l'installation d'un enregistreur de numéros de téléphone, prévue à l'article 492.2 C.cr., supporte, dans une certaine mesure, la proposition selon laquelle plusieurs informations ne présentant pas, à leur face même, de caractère biographique d'ordre personnel, doivent bénéficier d'une certaine protection constitutionnelle. Il va toutefois sans dire, dans le cas qui nous intéresse, que les métadonnées des communications électroniques ne sauraient être assimilées à de simples « numéros de téléphone ». Voir W. N. RENKE, préc., note 84, 804.

[307] Derek Lai soutient que la vidéo surveillance continue et généralisée d'un secteur, de par sa simple portée, peut permettre l'obtention de renseignements biographiques d'ordre personnel sur certains individus : « […] we live much of our lives in public, and what we display reveals a considerable amount about our personal and lifestyle choices. A police officer who catches a quick glimpse of us might derive a tidbit of information. But systematic surveillance as we move through an area can collect a greater volume and range of information, especially if we happen to live and/or work in that area. No longer is the information distributed among many different parties. The camera can see who we meet with, where we go, and which things we buy. Those isolated pieces of information can be amalgamated in the hands of the state, enabling police to create a fairly complete picture of who we are and how we live. Thus, the mere scope of the information collected by street video surveillance means that it can intrude on a ''biographical core of information'' ». Voir Derek LAI, « Public Video Surveillance by the State : Policy, Privacy Legislation, and the Charter », (2007) 45-1 *Alta. L. Rev.* 43, 71.

[308] Nul ne saurait prétendre que l'emplacement à partir duquel un individu effectue un appel à l'aide de son appareil de téléphonie cellulaire en révèle autant, sur le plan de la vie privée, que ses préférences sexuelles. La situation n'est toutefois pas toujours aussi tranchée. À ce sujet, nous référons le lecteur au titre « 1.2.1.4. Le potentiel très révélateur des métadonnées ».

[309] *Supra*, 1.2.1.4.

renseignements que révèle l'analyse de masses de métadonnées agrégées se trouve exacerbée par la quantité effarante d'informations générées quotidiennement[310], de même que par les méthodes et techniques utilisées par l'État relativement à leur surveillance[311]. Ces trois facteurs que sont la quantité brute d'informations disponibles, l'approche adoptée par l'État quant à la surveillance et à la collecte à grande échelle des métadonnées des communications électroniques, ainsi que le caractère fondamentalement privé des renseignements qu'il est possible d'obtenir par le biais de leur analyse, nous incitent à considérer que ces métadonnées correspondent précisément à l'objet de ce que l'article 8 de la *Charte canadienne* vise à protéger.

La forme spécifique de l'atteinte à la vie privée que posent aujourd'hui les activités gouvernementales de surveillance électronique à grande échelle rend nécessaire un élargissement de la portée du cadre d'analyse du « Biographical core », de manière à tenir compte de la réalité technique de la surveillance. L'analyse des métadonnées recueillies dans le cadre de cette surveillance permet, lorsqu'elles sont agrégées, l'obtention de renseignements d'une nature fondamentalement privée, parfois même plus délicats que le contenu des communications ayant généré lesdites métadonnées en premier lieu. Or, il nous apparaît inacceptable, en 2014, que la technicité que constitue la distinction entre le contenu d'une communication et ses métadonnées se solde, dans le contexte qui nous intéresse, par une modulation de la protection constitutionnelle dévolue aux renseignements personnels. Une telle distinction n'est tout simplement plus valide.

---

[310] *Supra*, 1.2.1.3.
[311] *Supra*, 1.2.2.2 à 1.2.2.4.

3.1.1.2. La désuétude de la distinction contenu-métadonnée dans le contexte contemporain

Il y a une trentaine d'années, il n'était pas nécessaire que la protection conférée à la vie privée informationnelle vise également les métadonnées d'une communication, dans la mesure où il existait une distinction marquée entre le contenu de ladite communication et ses métadonnées, et ce, pour plusieurs raisons. Tout d'abord, le nombre de métadonnées associées à une communication était beaucoup plus limité et celles-ci n'étaient pas, dans la majorité des cas, générées à l'insu des individus concernés[312]. De plus, la limitation des capacités technologiques empêchait les autorités de procéder à la collecte, l'agrégation et l'analyse systématique et automatisée des communications, lesquelles n'étaient d'ailleurs pas, pour la plupart, électroniques ou numériques. Finalement, les métadonnées d'une communication étaient, en ce qui concerne le caractère privé de cette dernière, tout simplement beaucoup moins révélatrices que son contenu.

Or, nous sommes forcés de reconsidérer la validité de ces affirmations et de constater que la distinction contenu-métadonnées ne correspond désormais plus adéquatement à la réalité technologique contemporaine. Ainsi, comme nous l'avons expliqué dans la première partie de ce mémoire, il n'existe pas de séparation nette entre le contenu d'une communication électronique et ses métadonnées[313]. À partir du moment où il est établi que l'analyse des métadonnées des communications électroniques permet d'obtenir, à tout le moins, les mêmes renseignements personnels de nature biographique que ce à quoi il serait possible d'accéder en

[312] Par exemple, les métadonnées associées à l'envoi d'une communication postale étaient inscrites manuellement par l'expéditeur, en plus d'être limitées aux informations sommaires permettant l'identification des individus concernés et leurs adresses.
[313] *Supra*, 1.2.1.2.

interceptant directement le contenu desdites communications, cette distinction perd, sur les plans opérationnel et juridique, de sa pertinence. À la lumière de l'ensemble de ces éléments, le modèle d'analyse du caractère privé d'un renseignement repose de moins en moins sur la distinction contenu-métadonnée, à la faveur d'une appréhension fondée sur le modèle du continuum[314]. La désuétude de cette distinction illustre très bien, selon nous, les risques que présente toute tentative de catégorisation hâtive de la nature des renseignements personnels, dans le contexte de l'utilisation des nouvelles technologies de l'information et des communications, et ce, particulièrement en ce qui concerne les métadonnées des communications électroniques. Tel que nous le verrons désormais, les enseignements de la Cour suprême du Canada semblent, à cet égard, déterminants.

3.1.1.3. La qualité intrinsèque des renseignements visés par la surveillance électronique gouvernementale

La Cour suprême s'est récemment prononcée avec vigueur, dans l'arrêt *R.* c. *Spencer*[315], analysé dans la deuxième partie de ce mémoire[316], sur la qualification et la catégorisation des renseignements, eu égard à leur caractère privé, dans le cadre de la détermination de l'objet d'une fouille, perquisition ou saisie en matière de vie privée informationnelle. Dans cet arrêt, la cour a jugé, nous le rappelons, qu'il était nécessaire, de « tenir compte de la tendance qui consiste à chercher à obtenir des renseignements pour permettre d'en tirer des inférences au

---

[314] Dans cet ordre d'idées, voir les propos très éloquents de Michael Morell, rapportés par J. SANCHEZ, préc., note 79.
[315] *R.* c. *Spencer*, préc., note 186.
[316] *Supra*, 2.2.3.

sujet d'autres renseignements qui, eux, sont de nature personnelle »[317]. Cette position de la cour est absolument fondamentale à notre argumentation, dans la mesure où elle nous permet de soutenir que les métadonnées des communications électroniques constituent des « renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu », au sens de l'arrêt *R.* c. *Plant*[318]. Ainsi, malgré le fait que ces métadonnées ne présentent généralement pas, à leur face même, de caractère « biographique d'ordre personnel », il nous semble évident qu'elles peuvent aisément fournir, suite à leur collecte à grande échelle, leur agrégation et leur analyse, un portrait très intime des individus visés. Ce faisant, ces métadonnées permettent indéniablement aux autorités, selon les termes mêmes de la Cour suprême, dans l'arrêt *R.* c. *Spencer*, de « tirer des inférences au sujet d'autres renseignements qui, eux, sont de nature personnelle »[319]. Il en découle que le point focal de toute analyse portant sur la détermination de l'existence d'intérêts privés en matière informationnelle doit être centré sur la qualité intrinsèque des renseignements étudiés et leur potentiel eu égard à la révélation d'informations de nature personnelle[320]. Ce raisonnement nous semble tout à fait conforme à la jurisprudence constitutionnelle ayant établi que l'atteinte au droit à la vie privée causée par toute fouille, perquisition ou saisie doit être appréhendée en fonction de ses conséquences sur les individus touchés[321]. Ceci implique donc, tel que précisé dans *R.* c. *Spencer*, de se concentrer sur « la nature des droits en matière de vie privée auxquels l'action de l'État [est susceptible de] porter atteinte »[322].

---

[317] *R.* c. *Spencer*, préc., note 186, par. 31.
[318] *R.* c. *Plant*, préc., note 238, 293.
[319] *R.* c. *Spencer*, préc., note 186, par. 31.
[320] *R.* v. *Trapp*, préc., note 277, par. 37.
[321] *R.* c. *Evans*, préc., note 275, par. 11.
[322] *R.* c. *Spencer*, préc., note 186, par. 31.

À la lumière de cette démonstration, les éléments analysés nous semblent favorables à ce que le cadre d'analyse du « Biographical core » soit élargi, de manière à protéger les métadonnées des communications électroniques, appréhendées comme un tout. Comme il fut démontré, l'analyse informatisée de ces dernières permet l'obtention de renseignements indéniablement visés par l'essence même du « Biographical core ». Qui plus est, rien ne saurait justifier, en fonction de ce qui précède, le maintien de la distinction traditionnelle entre le contenu des communications électroniques et leurs métadonnées, ainsi que la modulation de la protection juridique à laquelle ces dernières ont droit. C'est d'autant plus vrai lorsque l'on considère le fait que l'analyse de ces métadonnées permet de tirer des inférences au sujet d'autres renseignements, lesquels sont personnels. L'environnement technologique actuel, conjugué à la nature et à l'étendue des pratiques de surveillance gouvernementale, nécessite que nous fassions preuve de flexibilité quant à l'appréhension du cadre d'analyse du « Biographical core »[323]. L'analyse de l'interprétation de l'article 8, dans le contexte des métadonnées des communications électroniques, appuiera fermement notre position à cet égard.

3.1.2. L'interprétation de l'article 8 au regard de l'environnement technologique contemporain

Maintenant que nous avons établi que les métadonnées des communications électroniques présentent un caractère fondamentalement privé, nous démontrerons que les

[323] À ce propos, Teresa Scassa écrit que « [b]ecause of the growing ease with which apparently innocuous information can be linked to and matched with other data, a more flexible approach to assessing the privacy interest in information is warranted. A single piece of information can convert anonymous data into highly sensitive personal information about identifiable individuals » (nos soulignements). Voir T. SCASSA, préc., note 240, 200-201.

principes d'interprétation propre à l'article 8 de la *Charte canadienne* appuient directement notre position selon laquelle la portée du « Biographical core » doit être élargie au regard de ces métadonnées. Cette incursion sur le terrain de l'interprétation nous permettra de traiter notre argumentaire avec concision et réalisme, sans nous égarer. Ainsi, nous ciblerons, dans un souci de concision, les décisions judiciaires nous apparaissant les plus pertinentes[324]. Pour ce faire, nous analyserons, tout d'abord, les grandes lignes du raisonnement fondant le recours, par la Cour suprême, à la méthode d'interprétation téléologique de l'article 8 de la *Charte canadienne* (3.1.2.1), avant de démontrer en quoi cette interprétation tend à favoriser la reconnaissance d'une sphère privée, dans le contexte de l'utilisation des nouvelles technologies de l'information et des communications (3.1.2.2). Précisons, par ailleurs, que l'exercice d'interprétation d'une disposition de la *Charte canadienne* aura lieu, dans le cadre d'un recours fondé sur celle-ci, à l'étape de l'analyse de l'existence d'une atteinte à un droit garanti[325].

3.1.2.1. L'interprétation téléologique de l'article 8 de la *Charte canadienne*

Il est aujourd'hui bien établi, tel que nous le verrons désormais, que l'article 8 de la *Charte canadienne* doit être interprété conformément à la méthode téléologique, donc en

---

[324] Bien que nous tentions, dans la mesure du possible, d'éviter les répétitions, il est possible que certains arrêts présentés ci-après, de même que les principes qui s'en dégagent, recoupent des éléments dont nous avons déjà traités, quoique dans un autre contexte.

[325] Le professeur Beaulac nous rappelle que le cadre d'analyse en deux temps d'un recours fondé sur la *Charte canadienne* fut établi dans les arrêts *R.* c. *Big M Drug Mart Ltd.*, préc., note 146 et *R.* c. *Oakes*, [1986] 1 R.C.S. 103. Ce cadre d'analyse prévoit, dans un premier temps, la détermination de l'existence d'une atteinte à un droit garanti, puis, dans un second temps, l'évaluation du caractère justifiable de l'atteinte, en vertu de l'article premier, dans le cadre d'une société libre et démocratique. Dans cet ordre d'idées, la détermination de l'existence d'une atteinte présuppose la délimitation de la portée de ce droit, par le biais d'une démarche interprétative. Voir Stéphane BEAULAC, *Précis d'interprétation législative. Méthodologie générale, Charte canadienne et droit international*, Montréal, LexisNexis, 2008, p. 385-386.

fonction de son objet, ses buts et sa finalité. Cette méthode d'interprétation, adoptée dès 1984 par la Cour suprême, dans l'arrêt *Hunter* c. *Southam Inc.*, commande une « analyse générale qui consiste à examiner le but visé et à interpréter les dispositions particulières d'un document constitutionnel en fonction de ses objectifs plus larges »[326]. Plus précisément, cette méthode peut être définie, en droit constitutionnel, comme une « forme de raisonnement par lequel le sens d'un texte juridique (par exemple, une règle, un principe ou autres normes) est déterminé en fonction de son but, son objet ou sa finalité »[327]. Elle rend nécessaire la détermination de l'objet d'une disposition afin d'être en mesure d'y donner son plein effet[328]. Un an après avoir adopté la méthode téléologique en matière d'interprétation des chartes, la Cour suprême a fourni d'importantes précisions quant à sa nature, dans l'arrêt *R.* c. *Big M Drug Mart* :

> Le sens d'un droit ou d'une liberté garantis par la *Charte* doit être vérifié au moyen d'une analyse de l'objet d'une telle garantie; en d'autres termes, ils doivent s'interpréter en fonction des intérêts qu'ils visent à protéger.
>
> À mon avis, il faut faire cette analyse et l'objet du droit ou de la liberté en question doit être déterminé en fonction de la nature et des objectifs plus larges de la *Charte* elle-même, des termes choisis pour énoncer ce droit ou cette liberté, des origines historiques des concepts enchâssés et, s'il y a lieu, en fonction du sens et de l'objet des autres libertés et droits particuliers qui s'y rattachent selon le texte de la *Charte*. Comme on le souligne dans l'arrêt *Southam*, l'interprétation doit être libérale plutôt que formaliste et viser à réaliser l'objet de la garantie et à assurer que les citoyens bénéficient pleinement de la protection accordée par la *Charte*. En même temps, il importe de ne pas aller au delà de l'objet véritable du droit ou de la liberté en question et de se rappeler que la *Charte* n'a pas été adoptée en l'absence de tout contexte et que, par conséquent, comme l'illustre l'arrêt de Cour *Law Society of Upper Canada c. Skapinker*, [1984] 1 R.C.S. 357, elle doit être située dans ses contextes linguistique, philosophique et historique appropriés.[329] (soulignements originaux)

---

[326] *Hunter* c. *Southam Inc.*, préc., note 137, 156.
[327] Luc B. TREMBLAY, « L'interprétation téléologique des droits constitutionnels », (1995) 29 *R.J.T.* 459, 462.
[328] Mélanie SAMSON, « Interprétation large et libérale et interprétation contextuelle : convergence ou divergence? », (2008) 49 *C. de D.* 297, 313.
[329] *R.* c. *Big M Drug Mart Ltd.*, préc., note 146, 344.

Il découle de ce passage fondamental que la méthode téléologique implique, lors de l'interprétation d'une disposition de la *Charte canadienne*, la prise en compte du contexte dans lequel elle fut adoptée, de même que de l'objet des droits et libertés y étant garantis et des intérêts qu'ils visent à protéger[330].

Dans le contexte de l'article 8 de la *Charte canadienne*, la Cour suprême s'est spécifiquement prononcée, pour la première fois, sur la question de l'interprétation de la garantie contre les fouilles, perquisitions et saisies abusives prévue à la *Charte canadienne*, dans l'arrêt *Hunter* c. *Southam Inc.* Elle y a établi que l'article 8 devait être interprété en fonction de son but, donc en recourant à la méthode téléologique. Concrètement, la cour a tout d'abord précisé le but de la *Charte canadienne*, soit de « garantir et de protéger, dans des limites raisonnables, la jouissance des droits et libertés qu'elle enchâsse» et « [d']empêcher le gouvernement d'agir à l'encontre de ces droits et libertés »[331]. Dans le même ordre d'idées, la cour a estimé qu'il était nécessaire, afin d'évaluer la portée de la garantie contre les fouilles, perquisitions ou saisies abusives prévue à l'article 8, donc leur caractère raisonnable ou abusif, de déterminer le but de cet article et de « délimiter la nature des droits qu'il vise à protéger »[332]. Après avoir étudié la protection historique conférée à la vie privée – dans sa dimension territoriale – par la common law britannique, la cour est allée plus loin en établissant que « le texte de l'article [8] ne le limite aucunement à la protection des biens ni ne l'associe au droit applicable en matière d'intrusion » et qu'il « garantit un droit général à la protection contre les

---

[330] Le professeur Beaulac avance que ce passage fut cité par la Cour suprême dans la majorité des affaires ayant trait à l'interprétation de la *Charte canadienne*. Voir S. BEAULAC, préc., note 325, p. 390.
[331] *Hunter* c. *Southam Inc.*, préc., note 137, 156.
[332] *Id.*, 157.

fouilles, les perquisitions et les saisies abusives »[333]. La cour a poursuivi son analyse en ajoutant, après s'être référée à la jurisprudence constitutionnelle américaine[334], que l'article 8 protège les personnes et non les lieux[335]. La cour a finalement conclu sur cette question en synthétisant le principe général devant sous-tendre toute démarche d'interprétation de l'article 8 :

> [I]l faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi.[336]

Cette dynamique de pondération au cœur du raisonnement de la cour dans l'arrêt *Hunter* c. *Southam Inc.* résulte de la nature des fondements historiques, politiques et sociaux inhérents à la protection contre les fouilles, perquisitions et saisies abusives, telle que consacrée par l'article 8 de la *Charte canadienne*. Son interprétation en sera, comme nous le verrons, forcément tributaire.

La Cour suprême a raffiné ce raisonnement, quatre ans plus tard, dans l'arrêt *R.* c. *Dyment*, dans lequel elle a accordé une place centrale à l'objet, ainsi qu'aux fins de la protection de la vie privée. Ainsi, elle s'est fondée sur l'importance de la vie privée pour l'individu, de même que sur le plan de l'ordre public, pour reconnaître que « l'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique »[337]. Encore une fois, il fut démontré, dans cet arrêt, que l'article

---

[333] *Id.*, 158.
[334] *Katz* v. *United States*, préc., note 164. Sur cet aspect, voir *supra*, 2.1.1.2.
[335] *Hunter* c. *Southam Inc.*, préc., note 137, 159.
[336] *Id.*, 159-160.
[337] *R.* c. *Dyment*, préc., note 134, 427-428.

8 reposait sur des justifications sortant du cadre strictement juridique et visait, essentiellement, à aménager l'étendue du pouvoir étatique dans la vie de tout un chacun, au cœur de toute société démocratique. Plusieurs autres arrêts participent de ce processus.

Nous n'aurions, par exemple, qu'à citer l'arrêt *R.* c. *Plant*, rendu en 1993, dans lequel la cour s'est fondée sur les valeurs sous-jacentes de dignité, d'intégrité et d'autonomie consacrées par l'article 8 pour accorder une protection à la vie privée informationnelle[338], ou encore à l'arrêt *R.* c. *Tessling*, rendu en 2004, dans lequel la cour a souligné que la protection prévue à l'article 8 est un « élément fondamental de la relation entre l'État et le citoyen »[339]. C'est d'ailleurs dans l'arrêt *Tessling* que la cour a explicitement reconnu que « [p]eu de choses revêtent autant d'importance pour notre mode de vie que l'étendue du pouvoir conféré à la police d'entrer dans la maison d'un citoyen canadien, de porter atteinte à sa vie privée et même à son intégrité corporelle sans autorisation judiciaire »[340]. La cour a par la suite indiqué, en 2008, dans l'arrêt *R.* c. *A.M.*, qu'il pouvait être utile de tenir compte, dans le cadre de l'interprétation de l'article 8, du « type de société dans laquelle les Canadiens ont choisi de vivre en adoptant la *Charte* »[341]. Bref, la cour a récemment très bien résumé la situation dans

---

[338] *R.* c. *Plant*, préc., note 238, 293.
[339] *R.* c. *Tessling*, préc., note 183, par. 12.
[340] *Id.*, par. 13.
[341] *R.* c. *A.M.*, préc., note 268, par. 35. L'allocution prononcée par le très honorable Pierre Elliott Trudeau, alors premier ministre du Canada, lors de la Cérémonie de proclamation, le 17 avril 1982, est susceptible d'apporter un certain éclairage sur ce point. Trudeau y a déclaré: « [j]e souhaite que sur cette lancée, notre pays accède également à la maturité politique. Qu'il devienne en plénitude ce qu'il ne devrait jamais cesser d'être dans le coeur et dans l'esprit des Canadiens: […] un Canada où chaque personne puisse vivre librement son destin, à l'abri des tracasseries et de l'arbitraire des pouvoirs publics ». Voir Pierre Elliott TRUDEAU, *Allocution lors de la Cérémonie de proclamation*, 17 avril 1982, en ligne : <http://www.collectionscanada.gc.ca/premiersministres/h4-4024-f.html> (dernière consultation le 18 février 2015).

l'arrêt *R.* c. *Spencer*, lorsqu'elle s'est prononcée sur l'interprétation téléologique de la *Charte canadienne* :

> La Cour insiste depuis longtemps sur la nécessité d'adopter, à l'égard de l'art. 8, une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère.[342]

Ces enseignements jurisprudentiels illustrent adéquatement les propos des professeurs Brun, Tremblay et Brouillet, selon lesquels l'interprétation téléologique d'un droit fondamental nécessite que l'on s'interroge sur sa raison d'être, son origine historique, sa place dans le contexte de la tradition juridique britannique, puis canadienne, ainsi que sur l'histoire politique et sociale dont il est issu[343]. Qui plus est, l'approche dynamique et évolutive d'interprétation de la Constitution, qui vise à favoriser l'adaptation des normes constitutionnelles à l'ensemble des éléments factuels n'existant pas lors de leur adoption[344], s'avère particulièrement pertinente dans le contexte de la protection contre les fouilles, perquisitions ou saisies abusives. Bref, nous estimons que toute analyse plus approfondie des principes entourant la méthode téléologique d'interprétation constitutionnelle serait, aux fins de notre réflexion, superflue. Nous démontrerons plutôt en quoi cette méthode d'interprétation téléologique de l'article 8 de la *Charte canadienne* favorise la reconnaissance d'une sphère privée dans le contexte de l'utilisation des nouvelles technologies de l'information et des communications.

---

[342] *R.* c. *Spencer*, préc., note 186, par. 15.
[343] Henri BRUN, Guy TREMBLAY et Eugénie BROUILLET, *Droit constitutionnel*, 6e éd., Cowansville, Yvon Blais, 2014, p. 1000.
[344] P. HOGG, préc., note 165, p. 36-26.

3.1.2.2. L'article 8 face aux nouvelles technologies de l'information et des communications : la reconnaissance d'une sphère privée

La Cour suprême du Canada eut l'opportunité, depuis l'entrée en vigueur de la *Charte canadienne*, de se prononcer sur l'application de l'article 8 à un large éventail de situations novatrices sur le plan technologique. Ces situations impliquent, dans les quelques cas que nous analyserons, le recours aux nouvelles technologies de l'information et des communications. Nous nous intéresserons donc ici à l'intégration, par la cour, de la dimension technologique à son raisonnement quant à l'interprétation de l'article 8. Pour ce faire, nous traiterons tout d'abord brièvement de l'approche interprétative adoptée eu égard à l'évolution technologique, dans sa globalité (3.1.2.2.1), avant de nous intéresser, plus spécifiquement, à son application dans le contexte des nouvelles technologies de l'information et des communications, ainsi qu'aux métadonnées des communications électroniques (3.1.2.2.2).

3.1.2.2.1. La prise en considération de l'évolution du contexte technologique

Il est possible d'affirmer, d'entrée de jeu, dû à la teneur des règles d'interprétation constitutionnelle et à la méthodologie propre à l'interprétation de l'article 8, que la garantie contre les fouilles, les perquisitions et saisies abusives est appelée à s'adapter au gré de l'évolution de la société et, plus particulièrement, à la complexification et au raffinement des outils utilisés par l'État pour y porter atteinte. Précisons tout d'abord, dans cet ordre d'idées, que la Cour suprême reconnait, depuis l'arrêt *R.* c. *Duarte*, le principe général selon lequel « la surveillance électronique d'un particulier par un organe de l'État constitue une fouille, une

perquisition ou une saisie abusive au sens de l'art. 8 de la *Charte* »[345]. C'est toutefois dans l'arrêt *R.* c. *Wong* que la cour a expressément affirmé, pour la première fois, qu'il devait être possible d'adapter la protection conférée par l'article 8 aux moyens technologiques dont l'État était susceptible de disposer dans l'avenir :

> Dans l'arrêt *Duarte*, cette Cour a conclu que la surveillance électronique audio non autorisée constitue une violation de l'art. 8 de la *Charte*. Il serait erroné de limiter les effets de cette décision à cette technologie particulière. Il faudrait plutôt conclure que les principes énoncés dans l'arrêt *Duarte* embrassent tous les moyens actuels permettant à des agents de l'État de s'introduire électroniquement dans la vie privée des personnes, et tous les moyens que la technologie pourra à l'avenir mettre à la disposition des autorités chargées de l'application de la loi.[346] (soulignements originaux)

Il est important de comprendre ici que l'article 8 a vocation à s'appliquer aux méthodes et techniques permettant aux agents de l'État d'effectuer des fouilles, perquisitions ou saisies sans égard à leur nature ou leur complexité technologique. Toujours dans l'arrêt *Wong*, la cour a poursuivi son analyse en se fondant sur les propos formulés en dissidence par le juge Louis Brandeis, dans l'arrêt rendu en 1928 par la Cour suprême des États-Unis, dans l'affaire *Olmstead v. United States*[347], selon lequel « il ne [faut] pas s'attendre à ce que les progrès de la science, qui fournissent au gouvernement les moyens de procéder à de "l'espionnage", s'arrêtent à l'écoute » et à l'effet que « les clauses qui assurent aux particuliers une protection contre des abus de pouvoir précis doivent être susceptibles d'adaptation à un monde en évolution »[348]. Après avoir référé aux principes d'interprétation de la *Charte canadienne*

---

[345] *R.* c. *Duarte*, préc., note 221, 42-43.
[346] *R.* c. *Wong*, préc., note 178, 43-44.
[347] *Olmstead* v. *United States*, [1928] 277 U.S. 438.
[348] *R.* c. *Wong*, préc., note 178, 44.

formulés dans l'arrêt *Hunter* c. *Southam Inc.*[349], la cour a conclu sur la question de l'adaptation de l'article 8 en ces termes non équivoques :

> Le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés.[350]

Ce passage, on ne peut plus clair quant à la capacité d'adaptation de l'article 8, est fondamental à notre argumentaire relativement à la portée du « Biographical core » et à la protection constitutionnelle des métadonnées des communications électroniques. Qui plus est, il synthétise adéquatement le fil conducteur de l'approche adoptée par la Cour suprême, depuis lors, concernant l'interprétation de l'article 8 dans les situations impliquant l'utilisation des nouvelles technologies de l'information et des communications.

3.1.2.2.2. Les nouvelles technologies de l'information et des communications et les métadonnées des communications électroniques

Il nous apparaît évident, à cette étape de notre raisonnement, que l'article 8 de la *Charte canadienne* doit être interprété d'une manière telle qu'il puisse protéger la vie privée des individus contre les atteintes étatiques, quelle qu'en soit la forme ou la sophistication. Pour ce faire, cet article est appelé à évoluer et à s'adapter aux changements perpétuels qui caractérisent notre société, à commencer par la démocratisation de l'utilisation des nouvelles technologies de l'information et des communications et, plus particulièrement, aux métadonnées des communications électroniques. Rappelons que les tribunaux canadiens n'ont

[349] *Hunter* c. *Southam Inc.*, préc., note 137.
[350] *R.* c. *Wong*, préc., note 178, 44.

pas eu, à ce jour, l'opportunité de trancher la question de la protection juridique de ces métadonnées, dans le contexte des activités gouvernementales de surveillance électronique à grande échelle dont elles font l'objet. Néanmoins, nous estimons être en mesure de soutenir le fait que les principes jurisprudentiels propres à l'interprétation de l'article 8 permettent d'élargir la portée du « Biographical core », de manière à reconnaître et protéger le caractère éminemment « biographique d'ordre personnel » des métadonnées des communications électroniques[351]. Ceci étant, la Cour suprême s'est penchée, dans les dernières années, sur plusieurs affaires dans lesquelles l'atteinte alléguée à l'article 8 résultait de la fouille, perquisition ou saisie de renseignements privés contenus sur des ordinateurs personnels et des téléphones cellulaires[352]. La cour a ainsi rendu, depuis 2010, trois arrêts d'une importance considérable eu égard à la portée de la protection de la vie privée informationnelle dans le contexte de l'utilisation d'un ordinateur personnel ou d'un téléphone cellulaire, dans les affaires *R.* c. *Morelli*[353], *R.* c. *Vu*[354] et *R.* c. *Société TELUS Communications*[355]. Les principes élaborés dans celles-ci participent à la reconnaissance d'une sphère privée dans le contexte de l'utilisation des nouvelles technologies de l'information et des communications, lesquels sont, tel que nous le démontrerons désormais, directement applicables aux métadonnées des communications électroniques.

---

[351] Sur ce dernier point, voir *supra*, 3.1.1.
[352] Nous concentrerons, dans un souci de concision, notre traitement de ces arrêts sur la nature des atteintes aux intérêts protégés par le droit à la vie privée, dans la perspective de l'adaptation des garanties de l'article 8 aux technologies que sont les ordinateurs personnels et les téléphones cellulaires. Nous reconnaissons toutefois qu'il eut été très intéressant de nous intéresser plus en profondeur aux arrêts présentés, ainsi que d'en inclure d'autres, notamment rendus par des tribunaux d'instances inférieures, et d'étudier chacun d'eux dans le détail. Néanmoins, l'approche que nous priorisons nous permettra de cibler exclusivement les éléments étant directement pertinents à notre argumentaire entourant la protection juridique des métadonnées.
[353] *R.* c. *Morelli*, [2010] 1 R.C.S. 253.
[354] *R.* c. *Vu*, [2013] 3 R.C.S. 657.
[355] *R.* c. *Société TELUS Communications*, [2013] 2 R.C.S. 3.

La Cour suprême a reconnu d'emblée, dans l'arrêt *Morelli*, qui portait sur la fouille et la saisie d'un ordinateur personnel, qu'« il est difficile d'imaginer une perquisition, une fouille et une saisie plus envahissantes, d'une plus grande ampleur ou plus attentatoires à la vie privée que celles d'un ordinateur personnel »[356]. Cette position se trouve à être justifiée par le caractère sensible et éminemment privé des renseignements susceptibles d'être contenus dans un ordinateur personnel :

> Nos ordinateurs contiennent souvent notre correspondance la plus intime. Ils renferment les détails de notre situation financière, médicale et personnelle. Ils révèlent même nos intérêts particuliers, préférences et propensions, enregistrant dans l'historique et la mémoire cache tout ce que nous recherchons, lisons, regardons ou écoutons dans l'Internet.[357]

Cet extrait illustre le fait que la cour soit disposée à reconnaître clairement l'existence d'une sphère privée dans le cadre de l'utilisation des nouvelles technologies de l'information et des communications, telles qu'elles sont actuellement disponibles. C'est d'ailleurs précisément le caractère intime des renseignements contenus sur un ordinateur personnel qui a incité la cour à soutenir qu'il était difficile de « concevoir une violation de l'art. 8 ayant des répercussions plus graves [que la fouille d'un ordinateur personnel] sur le droit à la protection de la vie privée que la Charte garantit »[358]. Il est, selon nous, possible d'en dire autant des métadonnées des communications électroniques. Comme nous l'avons vu, l'agrégation et l'analyse de ces métadonnées permet l'obtention d'une quantité importante de renseignements de nature intrinsèquement privée. Il nous semble donc raisonnable de croire que le raisonnement de la cour eu égard à l'importance de l'atteinte résultant d'une fouille,

---

[356] *R.* c. *Morelli*, préc., note 353, par. 2. La cour ajoute, au paragraphe 106, que l'« [o]n peut […] difficilement concevoir une violation de l'art. 8 ayant des répercussions plus graves sur le droit à la protection de la vie privée que la Charte garantit ».

[357] *Id.*, par. 105.

[358] *Id.*, par. 106.

perquisition ou saisie en matière d'ordinateurs personnels – dans la mesure où ce raisonnement est fondé sur le caractère hautement privé des renseignements y étant contenus – est applicable aux métadonnées des communications électroniques. Dans cet ordre d'idées, la violation du droit à la vie privée découlant de la surveillance électronique et de la collecte de ces métadonnées nous apparaît au moins aussi attentatoire que la fouille, perquisition ou saisie du contenu d'un ordinateur personnel.

La Cour suprême s'est par la suite spécifiquement penchée, en 2013, dans l'arrêt *R.* c. *Vu*[359], sur l'actualisation du cadre juridique traditionnel régissant le droit des fouilles, perquisitions et saisies, dans l'objectif avoué de « protéger les intérêts uniques en matière de vie privée que met en jeu la fouille des ordinateurs »[360]. Elle y a établi qu'il était nécessaire, pour les autorités, d'obtenir une autorisation expresse préalablement à la fouille d'ordinateurs[361] dû au fait qu'ils « sont susceptibles de donner aux policiers accès à de vastes quantités de données sur lesquelles les utilisateurs n'ont aucune maîtrise, dont ils ne connaissent peut-être même pas l'existence ou dont ils peuvent avoir choisi de se départir, et qui d'ailleurs pourraient fort bien ne pas se trouver concrètement dans le lieu fouillé »[362]. En approfondissant son raisonnement relativement à la différence entre les « contenants » traditionnels[363] et les ordinateurs, la cour a insisté sur le fait que, parmi l'immense quantité de données stockées sur un ordinateur, certaines étaient susceptibles d'être visées par le «

[359] *R.* c. *Vu*, préc., note 354.
[360] *Id.*, par. 1-2.
[361] *Id.*, par. 20.
[362] *Id.*, par. 24.
[363] Par exemple, les classeurs, boîtes et autres outils de rangement documentaire du même acabit.

Biographical core »[364]. Qui plus est, des données sont générées automatiquement, souvent « à l'insu de l'utilisateur »[365] et conservées même si celui-ci croit les avoir détruit[366]. Ces éléments ont incité la cour à reconnaître, comme elle l'avait précédemment fait dans l'arrêt *Morelli*, que les ordinateurs personnels nécessitent une protection juridique accrue dû à la sensibilité et au caractère potentiellement privé des renseignements qu'ils contiennent et au fait que leurs utilisateurs bénéficient à l'égard de ces ordinateurs d'une attente raisonnable en matière de vie privée[367]. Encore une fois, plusieurs éléments ayant influencé la position de la cour dans cet arrêt sont directement applicables aux métadonnées des communications électroniques. Ainsi, celles-ci sont susceptibles, au même titre que les données contenues sur les ordinateurs personnels, de donner accès aux autorités à une importante quantité de renseignements de nature privée, sur lesquels les utilisateurs n'ont généralement aucun contrôle et dont ils ne connaissent pas l'existence, dans la mesure où ils sont, bien souvent, générés à son insu[368]. Advenant le cas où l'utilisateur serait conscient que des métadonnées sont générées suite à l'envoi ou à la réception d'une communication électronique et, conséquemment, déciderait de

---

[364] *R.* c. *Vu*, préc., note 354, par. 41.

[365] *Id.*, par. 42.

[366] *R.* c. *Vu*, préc., note 354. La cour ajoute par ailleurs que « [l]es ordinateurs compromettent ainsi de deux façons la capacité des personnes qui les utilisent de rester maîtres des renseignements disponibles à leur sujet : ils créent de l'information à l'insu des utilisateurs et ils conservent des données que ces derniers ont tenté d'effacer. En raison de ces caractéristiques, les ordinateurs sont fondamentalement différents des contenants que le droit relatif aux fouilles, perquisitions et saisies a dû régir par le passé » (par. 43).

[367] Il ne nous semble pas nécessaire d'aborder spécifiquement ce point, mais précisons que la cour a jugé, dans l'arrêt *R.* c. *Cole*, préc., note 265, qu'un individu bénéficie d'une attente raisonnable en matière de vie privée relativement à l'utilisation d'ordinateurs de travail, quoique celle-ci soit réduite par rapport aux ordinateurs personnels (par. 8-9).

[368] La plupart des individus seraient, par exemple, surpris d'apprendre que les métadonnées suivantes sont automatiquement générées lorsqu'un appel est effectué par le biais d'un appareil de téléphonie cellulaire : les numéros de téléphone de chaque participant à l'appel, les numéros de série uniques des téléphones utilisés, l'heure de l'appel et sa durée, l'emplacement géographique de chaque participant à l'appel, de même que les numéros de cartes téléphoniques des appareils utilisés. Sur ce point, voir GUARDIAN US INTERACTIVE TEAM, préc., note 76.

supprimer ladite communication, les métadonnées n'en seraient pas moins automatiquement conservées, à son insu, sur le réseau utilisé[369].

La cour a également précisé, dans l'arrêt *Vu*, que son raisonnement à l'égard des ordinateurs personnels était pleinement applicable aux téléphones cellulaires, essentiellement dû à l'évolution de leurs capacités :

> En ce qui a trait à l'autorisation préalable, je ne fais aucune distinction entre les ordinateurs et le téléphone cellulaire en litige dans la présente affaire. Il est vrai que, dans le passé, le volume et le genre de données qu'il était possible de stocker dans les téléphones cellulaires étaient bien plus limités que dans les ordinateurs, mais les cellulaires modernes disposent de capacités qui, pour les fins qui nous occupent, équivalent à celles des ordinateurs. La juge de première instance a conclu que, par exemple, le téléphone cellulaire saisi en l'espèce possédait [traduction] « une capacité de mémoire analogue à celle d'un ordinateur » […]. Par conséquent, lorsque je fais mention des « ordinateurs » dans les présents motifs, je vise également le téléphone cellulaire.[370]

Ainsi, s'il a pu être possible d'opérer, dans le passé, une distinction entre le traitement juridique des ordinateurs portables et des téléphones cellulaires en matière de protection de la vie privée informationnelle, l'évolution rapide de ces derniers rend aujourd'hui toute distinction de ce type beaucoup plus difficile à justifier.

La cour a, par ailleurs, clairement affirmé, dans l'arrêt *R.* c. *Société Telus Communications*, l'application aux téléphones cellulaires du principe établi dans l'arrêt *R.* c. *Wong*[371] à l'effet que « les droits garantis par l'art. 8 de la *Charte* […] doivent progresser au

---

[369] Le fait, par exemple, de supprimer un message électronique n'entraîne pas pour autant la suppression de l'ensemble des métadonnées qui y sont associées, lesquelles sont généralement archivées dans le système du fournisseur du réseau de communication, et ce, dès la transmission dudit message.

[370] *R.* c. *Vu*, préc., note 354, par. 38.

[371] *R.* c. *Wong*, préc., note 178.

rythme de la technologie »[372]. Dans l'arrêt *R.* c. *Société Telus Communications*, la cour a indiqué que la seule distinction existant entre une communication orale et une communication par le biais de la messagerie textuelle réside dans leur processus de transmission[373]. Ce faisant, la cour a précisé que « [l]es différences techniques intrinsèques des nouvelles technologies ne [doivent] pas déterminer l'étendue de la protection accordée aux communications privées »[374]. Cette position souligne adéquatement, selon nous, le fait que l'évolution technologique rapide a pour conséquence de centrer l'analyse de l'atteinte d'une fouille, perquisition ou saisie en matière informationnelle sur l'importance des renseignements visés et leur caractère potentiellement privé, plutôt que simplement sur le support sur lequel ils sont contenus. Cette position peut s'avérer bénéfique aux métadonnées des communications électroniques, dans la mesure où, tel que nous l'avons précédemment démontré[375], toute analyse visant à déterminer l'existence d'intérêts privés en matière informationnelle sera concentrée sur la qualité intrinsèque des renseignements en question et leur potentiel relativement à la révélation d'informations de nature personnelle[376].

Tous ces éléments confirment le fait que la Cour suprême semble consciente des risques que posent les fouilles, perquisitions ou saisies pour la vie privée dans l'environnement technologique d'aujourd'hui, de même que de la nécessité corrélative d'interpréter et

---

[372] *R.* c. *Société TELUS Communications*, préc., note 355. Dans cet ordre d'idées, la cour a reconnu que l'envoi de messages textes survient dans des circonstances faisait naître, chez les utilisateurs d'un téléphone cellulaire, une attente raisonnable en matière de respect de la vie privée (par. 32).
[373] *Id.*, par. 5.
[374] *Id.*
[375] *Supra*, 3.1.1.3.
[376] Voir *R.* v. *Trapp*, préc., note 277, par. 37; et *R.* c. *Spencer*, préc., note 186, par. 25-26 et 31-37.

d'adapter, avec souplesse, l'article 8 de la *Charte canadienne* face à cette nouvelle réalité[377]. Par ailleurs, bien que la cour ait récemment jugé, dans l'arrêt *R.* c. *Fearon*[378], que le pouvoir de common law régissant les fouilles accessoires autorisait les autorités policières à fouiller le téléphone cellulaire d'un prévenu, la majorité des juges a expressément rappelé le principe selon lequel « [l]es téléphones cellulaires […] mettent en cause des intérêts importants en matière de respect de la vie privée »[379].

Bien qu'il eut théoriquement été possible d'inférer, en nous fondant strictement sur les principes généraux d'interprétation constitutionnelle et sur ceux propres à l'article 8 de la *Charte canadienne*, que la protection conférée à la vie privée par cette disposition évoluerait au gré de la technologie, la jurisprudence analysée illustre la détermination avec laquelle la Cour suprême a entrepris d'adapter cette protection à la réalité technologique contemporaine. L'ensemble de ces éléments nous permet également de croire que la méthode propre à l'interprétation de l'article 8, particulièrement à la lumière des arrêts de la Cour suprême dans les affaires *Morelli*, *Vu* et *Société Telus Communications*, est aujourd'hui favorable à la reconnaissance d'une sphère privée dans le contexte de l'utilisation des nouvelles technologies de l'information et des communications. Elle nous semble également tout à fait favorable à un

---

[377] Une telle interprétation de l'article 8 est fondamentalement incompatible avec la détermination préalable d'un ensemble de techniques d'enquête autorisées ou prohibées, tel que l'a jugé la Cour suprême dans l'arrêt *R.* c. *Tessling*, préc., note 183: « [é]tant donné l'ensemble déconcertant de techniques différentes (existantes ou en développement) qui s'offrent à la police, il ne serait guère réaliste d'appliquer [une] méthode consistant à établir un « catalogue » judiciaire de ce qui est ou n'est pas permis par l'art. 8 » (par. 19).

[378] *R.* c *Fearon*, 2014 CSC 77.

[379] *Id.*, par. 53. Précisons que cet arrêt n'est pas susceptible d'influencer notre raisonnement, dans la mesure où il porte sur la fouille du contenu d'un téléphone cellulaire et non sur les métadonnées des communications électroniques y étant associées, lesquelles ne sont d'ailleurs pas contenues sur le disque dur de l'appareil d'un individu, mais plutôt sur les serveurs des fournisseurs de services utilisés lors de leur génération (téléphonie cellulaire, messagerie électronique, etc.). Qui plus est, cet arrêt concerne l'interprétation d'un pouvoir prévu par la common law, applicable spécifiquement et exclusivement aux individus arrêtés. *À contrario*, notre réflexion vise les activités de surveillance généralisées ne ciblant aucun individu particulier.

élargissement de la portée du « Biographical core », de manière à reconnaître, de pair avec notre traitement de leur caractère fondamentalement personnel[380], une certaine protection juridique aux métadonnées des communications électroniques. Cette approche nous apparaît conforme à l'objet de l'article 8, à savoir la protection du droit à la vie privée de tout un chacun, ainsi que l'aménagement des rapports entre l'État et l'individu. Ce faisant, il est tout à fait logique que son interprétation tienne compte de l'évolution de la société et des moyens technologiques susceptibles d'être utilisés pour y porter atteinte.

Bref, nous estimons avoir démontré, dans cette sous-partie, qu'un élargissement de la portée du cadre d'analyse du « Biographical core » s'impose, de manière à assurer une protection constitutionnelle aux métadonnées des communications électroniques, lesquelles, lorsque prises individuellement, ne présentent pas forcément de caractère privé, mais dont l'agrégation rend toute analyse profondément attentatoire et susceptible de révéler des renseignements indéniablement personnels.

Plus précisément, nous considérons que les règles propres à l'interprétation constitutionnelle de l'article 8 de la *Charte canadienne* sont favorables à la reconnaissance d'une protection significative aux métadonnées des communications électroniques. Ce constat s'appuie sur la flexibilité et l'ouverture dont les tribunaux font systématiquement preuve lorsqu'ils interprètent l'article 8, particulièrement au regard de l'évolution technologique rapide caractérisant la société contemporaine. Il s'appuie également, comme nous l'avons vu, sur la nature fondamentalement personnelle, intime et privée des métadonnées des

[380] *Supra*, 3.1.1.

communications électroniques, dans le contexte de leur surveillance, leur collecte à grande échelle et leur analyse par les autorités gouvernementales.

Concrètement, l'élargissement de la portée du « Biographical core » serait pertinent à deux niveaux : il permettrait, d'une part, de conclure au caractère objectivement raisonnable d'une attente subjective en matière de vie privée à l'égard des métadonnées des communications électroniques, mais également, d'autre part, de conclure à leur caractère privé. Plus précisément, un tel élargissement rendrait ces métadonnées dignes d'être protégées en vertu de l'article 8. Il n'aurait pas pour conséquence directe d'interdire catégoriquement toute surveillance étatique les visant, mais plutôt d'influer sur la manière dont elles sont prises en compte, dans le cadre de l'analyse de l'ensemble des circonstances que commande l'article 8, à savoir à titre de renseignements biographiques d'ordre personnel et non plus comme de banales informations. L'interprétation de l'article 8 de la *Charte canadienne* que nous proposons aurait donc pour conséquence de catégoriser les actes invasifs de l'État à l'encontre des métadonnées – et des renseignements personnels qu'elles révèlent – comme étant des « fouilles, perquisitions ou saisies » devant être assujetties aux exigences que prévoit l'article 8.

Qui plus est, il nous semble évident que l'élargissement de la portée du « Biographical core » participe pleinement, dans l'environnement technologique contemporain, à la protection et à la préservation des valeurs promues par le concept même de vie privée informationnelle, à savoir la dignité, l'intégrité et l'autonomie de tout individu. Il nous semble tout aussi évident que l'obtention des renseignements personnels, que rendent possible la collecte et l'analyse des métadonnées des communications électroniques, constitue une violation de l'objet de la

protection de la vie privée informationnelle, puisqu'il en résulte un amoindrissent de l'autonomie, ainsi qu'un dévoilement de la personnalité des individus visés[381].

Quoi qu'il en soit, malgré l'état actuel du droit constitutionnel canadien, de la jurisprudence pertinente et de ce qu'il est possible d'en inférer, nous sommes forcés d'en venir à la conclusion que notre question de recherche, de par la complexité et le caractère profondément politique, voire social, des implications qu'elle soulève, ne saurait être étudiée en vase clos. L'indéniable attrait du prisme juridique ne nous dispense donc pas d'analyser le contexte global à la lumière duquel notre réflexion sera, ultimement, appréhendée.

3.2. La surveillance des métadonnées des communications électroniques au sein du contexte global

L'analyse constitutionnelle de la portée des droits fondamentaux et de la justification des atteintes gouvernementales constitue, nous en convenons, l'élément central de toute réflexion portant sur l'encadrement juridique des activités étatiques de surveillance. Nous sommes toutefois pleinement conscients du fait que l'appréhension réaliste et objective des enjeux soulevés dans le cadre d'une telle réflexion nécessite la prise en compte d'un ensemble de considérations non juridiques. Une telle démarche présuppose également que le droit, en plus d'être le fruit d'un consensus social, se trouve à directement – et durablement – affecter l'ensemble des processus sociaux. Cet entrelacement nous incite donc à intégrer à notre réflexion plusieurs considérations d'ordre politique, social et philosophique nous apparaissant

[381] GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, préc., note 187, p. 14.

essentielles au maintien du caractère démocratique de la société canadienne. Ce faisant, nous ciblerons, dans un premier temps, quelques-uns de ces facteurs (3.2.1), avant de traiter, très brièvement et de manière complémentaire, du fait que notre réflexion s'inscrit pleinement dans une discussion planétaire portant sur la surveillance électronique à grande échelle des métadonnées des communications électroniques (3.2.2).

3.2.1. Les implications sociales de la surveillance électronique des métadonnées

Il est essentiel, dans le cadre de notre réflexion, de nous questionner sur la nature des enjeux que soulèvent les activités gouvernementales de surveillance électronique à grande échelle des métadonnées, ainsi que leur ampleur. Nous avons donc ciblé quelques éléments présentant une pertinence accrue, au regard de notre raisonnement relativement à la protection juridique des métadonnées des communications électroniques[382]. Ce faisant, nous aborderons tout d'abord la question de l'équilibre entre le maintien de la sécurité nationale et la protection des droits fondamentaux (3.2.1.1), avant de traiter du caractère profondément invasif de l'infrastructure de surveillance électronique gouvernementale (3.2.2.2), puis du potentiel d'abus qui en résulte (3.2.2.3) et, finalement, des risques inhérents pour la vie privée (3.2.2.4).

3.2.1.1. L'équilibre entre le maintien de la sécurité nationale et la protection des droits fondamentaux

Précisons, d'entrée de jeu, que la surveillance, quelle que soit sa nature et son intensité, soulève des questions d'une importance fondamentale sortant de la sphère juridique. Il existe

[382] Nous n'entretenons, par souci de concision, aucune prétention d'exhaustivité à l'égard de ces éléments.

toutefois plusieurs distinctions juridiques majeures entre la surveillance policière traditionnelle et la surveillance gouvernementale à des fins de sécurité nationale, à commencer par leur encadrement législatif. Alors que les enquêtes policières sont menées en vertu du régime prévu au *Code criminel*[383], les activités de surveillance à des fins de sécurité nationale le sont généralement en vertu de la *Loi sur le service canadien du renseignement de sécurité*[384] et, en ce qui concerne leur dimension électronique, en vertu de la *Loi sur la défense nationale*[385]. La distinction la plus importante entre ces régimes, en ce qui nous concerne, réside toutefois dans le caractère considérablement plus attentatoire de la surveillance électronique gouvernementale à grande échelle des métadonnées des communications électroniques, laquelle vise de virtuellement tout individu, par opposition aux enquêtes policières, dont la portée est beaucoup plus restreinte. Ainsi, le caractère systémique des activités de surveillance visant ces métadonnées décuple l'ampleur de l'atteinte étatique aux droits et libertés fondamentaux, à un point tel que ces activités sont susceptibles de rompre le fragile équilibre démocratique entre le maintien de la sécurité nationale et la protection des droits individuels[386]. À ce sujet, la très honorable Beverley McLachlin avançait, en 2009, que :

> Le Canada a élaboré une approche qui lui est propre pour faire face aux défis créés par le terrorisme, une approche fondée sur la primauté des droits et sur le principe que l'État ne peut porter atteinte à ces droits que s'il est en mesure de justifier de telles restrictions. Nous reconnaissons la gravité de la menace que pose le terrorisme et la nécessité de le combattre avec vigilance. Mais nous reconnaissons

---

[383] *Code criminel*, préc., note 97, partie VI.
[384] *Loi sur le Service canadien du renseignement de sécurité*, préc., note 125, art. 12 à 20.
[385] *Loi sur la défense nationale*, préc., note 120, art. 273.61 à 273.7.
[386] Certaines pratiques policières plus « traditionnelles » contribuent également très certainement à ce phénomène, mais il ne nous semble pas pertinent d'apporter ici plus de précisions sur ce point.

> également qu'il faut porter le moins possible atteinte aux droits fondamentaux et que les effets de telles atteintes doivent être proportionnés.[387]

Ainsi, la primauté du droit et le caractère démocratique du système juridique canadien impliquent que l'on doive chercher à préserver l'équilibre entre le maintien de la sécurité et la protection des droits et libertés fondamentaux. Cette dynamique d'équilibration, au cœur du mécanisme constitutionnel d'évaluation de toute atteinte à la vie privée en vertu de l'article 8 de la *Charte canadienne*[388], caractérise également le processus politique canadien, dans le cadre duquel sont débattues et adoptées l'ensemble des mesures gouvernementales de sécurité nationale potentiellement attentatoires aux droits et libertés fondamentaux. Dans cet ordre d'idées, la juge en chef du Canada estime que :

> Dans toute réponse au terrorisme, le pouvoir législatif doit être le premier à intervenir. Les députés dûment élus doivent établir clairement les règles selon lesquelles le terrorisme est combattu. Ils doivent fixer la délicate ligne de démarcation entre la lutte contre le terrorisme et la préservation des libertés d'une façon qui soit efficace, constitutionnelle et donnent des indications claires à ceux qui sont chargés de combattre le terrorisme sur le terrain.[389]

Il est crucial que l'emphase soit mise, dans le cadre de ce processus législatif, sur l'objectivité et la proportionnalité, faute de quoi il existe un risque bien réel de prioriser la sécurité nationale, au détriment des valeurs mêmes que son maintien vise, en premier lieu, à protéger. La Cour suprême du Canada a parfaitement synthétisé cette problématique, dans l'arrêt *Suresh* c. *Canada (Ministre de la Citoyenneté et de l'Immigration)* :

> D'un côté, il y a le fléau manifeste du terrorisme et le meurtre gratuit et arbitraire de personnes innocentes, situations qui nourrissent l'engrenage de la destruction

---

[387] Beverley MCLACHLIN, *Lutter contre le terrorisme tout en préservant nos libertés civiles*, allocution prononcée devant le Ottawa Women's Canadian Club, 22 septembre 2009, en ligne : <http://www.scc-csc.gc.ca/court-cour/judges-juges/spe-dis/bm-2009-09-22-fra.aspx> (dernière consultation le 18 février 2015).

[388] Sur cette question, voir, en termes généraux, l'arrêt *Hunter* c. *Southam Inc.*, préc., note 137. Voir également *R.* c. *Genest*, préc., note 163, 63 et S. PENNEY, préc., note 163, 101-104.

[389] B. MCLACHLIN, préc., note 387.

> et de la peur. Pour exprimer la volonté des citoyens, les gouvernements ont besoin des outils juridiques propres à leur permettre de relever efficacement ce défi.
>
> De l'autre côté, il y a la nécessité de veiller à ce que ces outils juridiques ne sapent pas les valeurs jugées fondamentales par notre société démocratique — liberté, primauté du droit et principes de justice fondamentale — et qui sont au cœur de l'ordre constitutionnel canadien et des instruments internationaux dont le Canada est signataire. En effet, ce serait une victoire à la Pyrrhus que de vaincre le terrorisme au prix de notre adhésion à ces valeurs. Le défi du Parlement consiste à rédiger des lois qui combattent efficacement le terrorisme tout en respectant les exigences de notre Constitution et nos engagements internationaux.[390]

Il en découle, à notre avis, une nécessité de concilier le maintien de la sécurité nationale et la protection des droits fondamentaux, à commencer par la vie privée. D'où également l'importance de passer outre la dichotomie traditionnelle opposant ces deux éléments[391]. Ainsi, rappelons que plutôt que de s'inscrire dans cette dynamique d'opposition, le principe de pondération, au cœur de l'article 8 de la *Charte canadienne*, implique l'appréciation simultanée des intérêts étatiques et individuels[392]. Nous sommes toutefois forcés de constater, à la lumière du caractère profondément invasif des méthodes contemporaines de surveillance électronique, qu'un tel exercice s'avère relativement difficile.

3.2.1.2. Le caractère profondément invasif de l'infrastructure de surveillance contemporaine

Il est aujourd'hui indéniable que les gouvernements occidentaux, incluant le Canada, ont développé, grâce à l'innovation technologique, une formidable infrastructure de surveillance

---

[390] *Suresh* c. *Canada (Ministre de la Citoyenneté et de l'Immigration*, [2002] 1 R.C.S. 3, par. 3-4.

[391] Sur ce sujet, voir Laura K. DONOHUE, *The Cost of Counterterrorism. Power, Politics and Liberty*, Cambridge, Cambridge University Press, 2008. L'auteure y écrit, à la page 3 : « [t]he assumption is that security and freedom align on a fulcrum, so that elevating one ends the other plumetting toward the ground. The dichotomy assumes that, when threatened, a state may deprive individuals of certain rights. And it implicitely limits the range of choices to only two : security, on the one hand; on the other, freedom traded away. The assumptions are troubling. Some rights are fundamental to liberal democracy and cannot be relinquished ».

[392] *Hunter* c. *Southam Inc.*, préc., note 137, 159-160.

électronique[393]. Le sénateur américain Frank Church, qui eut, il y a plus d'une quarantaine d'années, l'opportunité d'étudier les activités de la *NSA*, affirma, relativement aux méthodes dont disposait alors l'agence de renseignement américaine, que « [t]hat capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide »[394]. L'essence de cet avertissement nous apparaît aujourd'hui prophétique, particulièrement à la lumière de l'accroissement exponentiel des capacités technologiques durant les quatre dernières décennies, ainsi que de la démocratisation des nouvelles technologies de l'information et des communications. Dans ce contexte, nul ne saurait s'étonner du caractère profondément invasif des activités gouvernementales de surveillance électronique des métadonnées des communications électroniques. Comme nous l'avons démontré dans ce mémoire, ce type de surveillance est très attentatoire pour la vie privée des individus, principalement dû à la nature technologique des méthodes et techniques utilisées. En effet, l'informatisation et l'automatisation des processus de collecte, d'analyse et d'archivage des renseignements personnels ciblés par l'infrastructure de surveillance étatique décuplent potentiellement l'ampleur et la gravité de toute violation injustifiée du droit à la vie privée des citoyens canadiens visés. Bien que les métadonnées collectées ne soient pas – faute de moyens et de temps – systématiquement passées au crible par des analystes humains, certains algorithmes permettent le traitement, l'analyse, le classement et le stockage accéléré des masses considérables de renseignements recueillis.

---

[393] *Supra*, 1.2.

[394] James BAMFORD, « The Agency that could be Big Brother », *The New York Times* (25 décembre 2005), en ligne : <http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=all&_r=1&> (dernière consultation le 18 février 2015).

Par ailleurs, nous reconnaissons que cette automatisation peut, à première vue, sembler « rassurante » pour quiconque ne s'intéresse pas spécifiquement aux enjeux juridiques inhérents à la surveillance à des fins de sécurité, de même que pour les individus moins soucieux de la protection de leur vie privée. Cette « déshumanisation » du processus peut influer sur la perception qu'ont ceux-ci quant à la gravité de la violation de leur vie privée informationnelle : qu'elle soit potentielle ou perçue, elle peut paraître moins réelle, moins intime, moins attentatoire, mais surtout, plus abstraite, voire plus rationnelle. Il ne faut toutefois pas se leurrer. Qu'elle soit opérée « manuellement » par des agents de l'État, comme ce fut traditionnellement le cas, ou en grande partie informatisée et automatisée, la surveillance et la collecte à grande échelle des métadonnées des communications n'en demeure pas moins profondément invasive. De surcroît, la nature des méthodes et techniques de surveillance employées ne fait qu'accroître, en l'absence d'un encadrement approprié, le potentiel de dérapages, voire d'abus, inhérent aux technologies de surveillance actuellement disponibles. Nous nous pencherons sur ce point.

3.2.1.3. Le potentiel d'abus

La gravité des abus que permet l'infrastructure informatique rendant possible, en premier lieu, l'interception des métadonnées des communications électroniques, est directement corrélée à la quantité pharaonique de données quotidiennement collectées et stockées, ainsi qu'à la puissance et à la précision des outils d'analyse disponibles. N'oublions pas que ces derniers demeurent contrôlés, supervisés et opérés par une myriade de fonctionnaires et de contractants de toutes sortes et qu'à ce titre, ils sont assujettis, malgré leur extrême sophistication, à la faillibilité de leurs opérateurs. Les risques d'abus que présente,

pour l'intégrité du processus démocratique dans son ensemble, une telle concentration de pouvoir, sont bien réels.

Ils peuvent, par exemple, résulter de la commission d'actes délibérés commis par certains fonctionnaires ayant accès à l'infrastructure de surveillance électronique, comme lorsqu'il fut révélé, en 2013, que des employés de la *NSA* avaient utilisé les capacités de surveillance de leur employeur à des fins romantiques[395]. L'infrastructure de surveillance peut également être utilisée, dans son ensemble, de manière abusive, résultant en la violation de certains principes démocratiques fondamentaux. Nous n'aurions, par exemple, qu'à citer les récentes révélations indiquant que les agences britanniques de renseignements que sont le *MI5*, le *MI6* et le *GCHQ* s'adonnent régulièrement à l'interception de communications privilégiées entre les avocats et leurs clients, dans le cadre de procès soulevant des questions épineuses liées à la sécurité nationale[396]. Ceci étant, nous n'avons pas la naïveté de prétendre qu'un élargissement de la portée du « Biographical core » aurait le moindre impact sur les motivations qui poussent certains individus à user déraisonnablement de leur pouvoir ou à en abuser. La protection constitutionnelle des métadonnées aurait néanmoins comme conséquence directe de juridiquement et expressément limiter la manière dont peut être utilisée la formidable infrastructure gouvernementale de surveillance à leur égard. Ce faisant, il nous apparaît crucial que des normes constitutionnelles encadrent adéquatement et

---

[395] Andrea PETERSON, « LOVEINT: When NSA officers use their spying power on love interests », *The Washington Post* (24 août 2013), en ligne : <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/> (dernière consultation le 18 février 2015).

[396] Owen BOWCOTT, « UK intelligence agencies spying on lawyers in sensitive security cases », *The Guardian* (7 novembre 2014), en ligne : <http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq> (dernière consultation le 18 février 2015).

décisivement l'exercice des activités étatiques de surveillance électronique, dont l'opacité caractéristique, bien que nécessaire, rend difficile toute évaluation indépendante digne de ce nom.

Il existe d'ailleurs, même en l'absence de toute forme d'abus, qu'ils soient volontaires ou non, certains risques inhérents à l'existence d'activités informatisées de surveillance électronique à grande échelle. Il serait, par exemple, possible qu'un individu soit catégorisé de « suspect », sur la base de l'établissement injustifié – mais automatique – de corrélations entre certains faits observés et recueillis. Ce type de situation découle directement du fait qu'une quantité considérable de renseignements sont collectés et archivés pour une durée indéterminée, rendant possible l'interprétation de faits précis hors de leur contexte, à la lumière d'évènements avec lesquels ils ne sont aucunement liés, parfois même longtemps après leur survenance initiale. Dans le même ordre d'idées, il existe un danger réel que ces renseignements erronés deviennent partie intégrante des dossiers numériques gouvernementaux permanents identifiant les individus en question[397]. Bref, l'existence d'une telle infrastructure technologique de surveillance gouvernementale présente, de par sa nature même, certains risques importants pour la vie privée des individus en territoire canadien. Il nous semble important d'apporter quelques précisions sur cet aspect.

[397] L. K. DONOHUE, préc., note 391, p. 266-267.

3.2.1.4. Les risques pour la vie privée

Nous n'aborderons ici que très brièvement la question des impacts potentiels des activités gouvernementales de surveillance électronique à grande échelle des métadonnées sur la vie privée des individus concernés, dans la mesure où le présent mémoire y est spécifiquement consacré. Qu'il nous suffise toutefois de préciser que de telles activités sont susceptibles, si elles ne sont pas adéquatement encadrées et balisées, de provoquer, dans le futur, des conséquences significatives relativement à l'existence d'une quelconque vie privée informationnelle, dans le sens où nous l'entendons aujourd'hui[398]. Ainsi, elles ont la capacité d'entraver et de réduire la sphère de vie privée à laquelle chaque individu peut prétendre bénéficier, et ce, d'une manière incompatible avec toute conception le moindrement crédible de la démocratie libérale canadienne. En ce sens, elles pourraient très certainement nuire aux valeurs fondamentales dont la vie privée permet la préservation et l'exercice, qu'il s'agisse de l'intimité, la liberté, l'autonomie, l'aménagement de relations humaines significatives, de même que de la structuration, l'aménagement et la participation aux rapports sociaux essentiels en démocratie[399]. Dans une perspective complémentaire, rappelons également que toute atteinte systémique importante à l'article 8 de la *Charte canadienne* est susceptible de nuire à une panoplie d'autres droits fondamentaux, dans la mesure où la protection de la vie privée en assure l'exercice effectif[400].

---

[398] L'approche qui vise à prévenir, à tout prix, la commission d'actes terroristes, favorisée par les gouvernements occidentaux suite aux attentats de septembre 2001, participe de ce phénomène et contribue à nuire, à certains égards, au droit à la vie privée ainsi qu'aux intérêts qu'il protège. À ce sujet, voir A. DAVIES, préc., note 288, 263 et s.

[399] Pour plus de détails sur ces aspects, voir *supra*, 1.1.

[400] Nous n'aurions qu'à citer les libertés de conscience, de religion, de croyance, d'opinion, d'expression, d'assemblée, ou encore d'association. Voir W. N. RENKE, préc., note 84, 804.

En conclusion et malgré tout ce qui précède, nous reconnaissons l'importance et la pertinence de la mise en place de mesures strictes visant à détecter et prévenir la radicalisation, l'extrémisme et le terrorisme. Toutefois, ces mesures, telles que la surveillance électronique et la collecte à grande échelle des métadonnées des communications électroniques, ne doivent pas occulter les principes et idéaux démocratiques qu'elles visent, en tout premier lieu, à protéger. Il est donc crucial de tenir compte, dans le cadre de toute réflexion entourant les mesures de sécurité nationale et la surveillance, des implications sociales, politiques et philosophiques soulevées, de manière à permettre l'analyse rationnelle de l'ensemble des enjeux impliqués. À cet égard, nous avons choisi de prioriser quatre éléments particuliers illustrant certaines conséquences potentielles du maintien, dans leur forme actuelle, des activités gouvernementales de surveillance électronique des métadonnées des communications électroniques. Il nous aurait, par ailleurs, été possible de traiter d'une foule d'autres éléments, tels que l'efficacité des mesures de surveillance, le réaménagement de l'équilibre du pouvoir entre les branches législative, exécutive et judiciaire, l'exacerbation des tentions latentes entre certains groupes sociaux et l'État, le désavantage de plusieurs groupes minoritaires, l'atteinte aux relations diplomatiques, l'accroissement de la bureaucratie ou encore les entraves à l'activité commerciale nationale et internationale[401]. Quoi qu'il en soit, la prise en considération du contexte mondial dans lequel s'effectue notre réflexion est aussi importante que les implications sociales qu'elle soulève et, à ce titre, nous nous y intéresserons désormais.

[401] L. K. DONOHUE, préc., note 391, p. 25.

3.2.2. La surveillance électronique des métadonnées dans le contexte mondial

Notre démarche de recherche, de par sa nature, ne saurait être menée « en silo », à l'abri de tout contexte factuel. Ceci étant, les révélations effectuées par Edward Snowden, ont provoqué, sur la scène planétaire, un tollé et une opposition sans précédent, dans l'histoire moderne, à la surveillance gouvernementale opérée au nom de la prévention du terrorisme, en plus de susciter une foule de réactions, aussi diversifiées que nombreuses, tant à l'égard d'Edward Snowden[402] que de certaines pratiques de surveillance. Ces révélations ont, par la force des choses, acculé et forcé les gouvernements occidentaux à adopter une position essentiellement défensive, particulièrement face aux nombreuses critiques soulevées à leur égard. Elles ont également permis de contextualiser et de légitimer la discussion mondiale portant sur ces pratiques de surveillance. La réflexion proposée dans notre mémoire s'inscrit directement dans ce phénomène. Dans cet ordre d'idées, il nous apparaît crucial d'aborder, ne serait-ce que très brièvement, les considérations soulevées dans le cadre de cette discussion planétaire. Bien qu'extrinsèques à la perspective strictement canadienne et juridique de notre raisonnement, celles-ci contribuent, au même titre que notre traitement des implications sociales, à contextualiser, de manière appropriée, notre réflexion. Ceci étant, nous nous intéresserons tout d'abord à l'approche empruntée par les États-Unis (3.2.2.1), avant de nous pencher sur l'action des organisations non gouvernementales (ci-après, les « ONG ») (3.2.2.2),

---

[402] Alors que certains n'hésitent pas à le voir comme un héros, d'autres considèrent qu'il s'agit plutôt d'un traître. Un sondage AngusReidGlobal, réalisé en 2013, nous apprenait que 51% des Américains interrogés percevaient Edward Snowden comme un héros, alors que 49% estimaient qu'il avait trahi son pays. L'opinion des Britanniques et des Canadiens à cet égard était, quant à elle, beaucoup plus tranchée. Ainsi, 60% des Britanniques et 67% des Canadiens considéraient qu'il s'était comporté de manière héroïque. Voir Shachi KURL, *More Canadians, Britons & Americans view Edward Snowden as « hero » than « traitor »,* Angus Reid Global, 2013, en ligne : <http://www.angusreidglobal.com/wp-content/uploads/2013/10/2013.10.30-Snowden-Leaks.pdf> (dernière consultation le 18 février 2015).

puis sur l'innovation dont font preuve, eu égard à la vie privée, plusieurs entreprises et groupes oeuvrant dans le domaine technologique (3.2.2.3).

3.2.2.1. L'approche empruntée par les États-Unis d'Amérique

Certains États visés par les révélations d'Edward Snowden ont tenté, malgré leur position très critique à son égard, de rassurer leur population relativement à la nature et à l'étendue de leurs activités de surveillance électronique à grande échelle. Nous citerons ici, en exemple, le cas des États-Unis, le pays indéniablement le plus durement touché par ces révélations[403]. Dans cette optique, l'administration américaine a mis en place, en août 2013, le *President's Review Group on Intelligence and Communications Technologies*. Ce groupe a formulé, quatre mois plus tard, 46 recommandations portant sur la réforme des activités de surveillance électronique américaines, incluant la cessation de la collecte à grande échelle et de l'archivage des métadonnées en sol américain :

> We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.[404]

Plus récemment, le *USA Freedom Act*, un projet de loi fédéral américain qui avait précisément pour objectif de mettre fin à ce type d'activités, fut rejeté par le Sénat

---

[403] Bien qu'il eut été très intéressant d'analyser les réactions spécifiques – et variées – d'un nombre plus important d'États, une telle démarche ne nous apparaît pas nécessaire, d'autant plus que le cas des États-Unis nous semble, à lui seul, particulièrement éclairant.

[404] Richard A. CLARKE, Michael J. MORELL, Geoffrey R. STONE, Cass R. SUNSTEIN et Peter SWIRE, *Liberty and Security in a Changing World*, President's Review Group on Intelligence and Communications Technologies, 2013, p. 25, en ligne : <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> (dernière consultation le 18 février 2015).

américain[405]. Il est toutefois intéressant de noter que la Cour suprême des États-Unis a jugé, dans un arrêt unanime rendu en juin 2014, qu'il était nécessaire, pour les autorités policières, d'obtenir une autorisation judiciaire préalablement à la fouille du téléphone cellulaire d'un prévenu[406]. Sans pour autant nous étendre plus longtemps sur cet aspect, précisons que virtuellement tous les États industrialisés se sont, depuis juin 2013, positionnés et prononcés sur la surveillance électronique à grande échelle menée par le gouvernement américain et ses alliés des *Five Eyes*, contribuant, par le fait même, à enrichir la réflexion globale entourant les révélations d'Edward Snowden. Les organisations non gouvernementales y participent également.

3.2.2.2. Le positionnement des organisations non gouvernementales

Il n'est pas surprenant que la plupart des organisations non gouvernementales d'envergure se soient prononcées avec vigueur sur la question de la surveillance électronique à grande échelle, telle que révélée par Edward Snowden. Ainsi, plus de 40 ONG ont récemment collaboré, à l'initiative de l'*Electronic Frontier Foundation* (ci-après, l'« EFF »), *Access* et

---

[405] Ellen NAKASHIMA et Ed O'KEEFE, « Senate fails to advance legislation on NSA reform », *The Washington Post* (18 novembre 2014), en ligne : <http://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html> (dernière consultation le 18 février 2015). Ce projet de loi fut, par ailleurs, sévèrement critiqué, notamment pour sa faiblesse. À ce sujet, voir Evan GREER, « How the USA Freedom Act failed on all fronts », *The Guardian* (19 novembre 2014), en ligne : <http://www.theguardian.com/media-network/2014/nov/19/how-usa-freedom-act-failed-on-all-fronts> (dernière consultation le 18 février 2015), ainsi que Glenn GREENWALD, « Congress Is Irrelevant on Mass Surveillance. Here's What Matters Instead », *The Intercept* (19 novembre 2014), en ligne : <https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/> (dernière consultation le 18 février 2015).

[406] *Riley* v. *California*, [2014] 573 U.S. ___. La cour a considéré que les téléphones cellulaires étaient, de nos jours : « such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy » (p. 9). Elle a ajouté, plus loin que : « it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate » (p. 19).

Privacy International, à la rédaction d'un cadre d'analyse en treize principes permettant l'évaluation de la conformité des lois en matière de surveillance, de même que des technologies et techniques dans ce domaine, au regard du droit international des droits de la personne[407]. Dans le même ordre d'idées, Amnistie internationale a développé, puis rendu public, en novembre 2014, un outil logiciel nommé *Detekt*, permettant à l'utilisateur d'un ordinateur de détecter, dans son système, la présence de logiciels espions gouvernementaux[408]. L'EFF a, pour sa part, conçu et mis en ligne le projet *Surveillance Self-Defense*, qui vise à fournir à tous des trucs, des outils et des guides à teneur pédagogique détaillant, une étape à la fois, comment sécuriser tout processus de communication en ligne[409].

Qui plus est, rappelons que l'ACLU a publié, en février 2014, un rapport très enrichissant portant spécifiquement sur la question de la surveillance électronique à grande échelle et de la collecte des métadonnées des communications électroniques, auquel nous avons référé dans la première partie de ce mémoire[410]. Finalement, l'EFF a publié, en mai 2014, un rapport détaillant la position des plus importantes sociétés américaines oeuvrant dans

---

[407] ELECTRONIC FRONTIER FOUNDATION, « International Principles on the Application of Human Rights to Communications Surveillance » (mai 2014), en ligne : <https://en.necessaryandproportionate.org/> (dernière consultation le 18 février 2015). Le préambule de ce document énonce, notamment: « [b]efore public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to Communications Surveillance by States. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. […] Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing Communications Surveillance technologies and techniques of the State, the ability of the State to combine and organize information gained from different surveillance technologies and techniques, or the increased sensitivity of the information available to be accessed. The frequency with which States are seeking access to both communications content and metadata is rising dramatically, without adequate scrutiny ».

[408] AMNISTIE INTERNATIONALE, « New tool for spy victims to detect government surveillance » (20 novembre 2014), en ligne : <http://www.amnesty.org/en/news/new-tool-spy-victims-detect-government-surveillance-2014-11-20> (dernière consultation le 18 février 2015).

[409] ELECTRONIC FRONTIER FOUNDATION, « Surveillance Self-Defense », en ligne : <https://ssd.eff.org/en> (dernière consultation le 18 février 2015).

[410] C. CONLEY, préc., note 75.

le domaine des technologies, en ce qui concerne la divulgation des données de leurs utilisateurs face aux requêtes gouvernementales[411]. Bref, il est clair que les ONG contribuent activement à la discussion, sur la scène mondiale, entourant la surveillance électronique à grande échelle. Tel qu'il sera maintenant démontré, certaines entreprises y participent également depuis peu.

3.2.2.3. L'innovation technologique entrepreneuriale au service de la vie privée

Nous constatons que, depuis les révélations d'Edward Snowden, plusieurs entreprises ou regroupements oeuvrant dans le domaine des nouvelles technologies ont su tirer profit de l'émergence d'une importante demande, dans les sociétés occidentales industrialisées, pour des services et dispositifs technologiques respectueux de la vie privée de leurs utilisateurs. Ainsi, *Silent Circle* offre à ses clients le *Blackphone*, un appareil mobile conçu et développé conjointement avec *Geeksphone*, dans l'objectif avoué de protéger le caractère privé des communications téléphoniques[412]. *Silent Circle* offre également, à titre complémentaire, une panoplie de forfaits téléphoniques et d'applications développées dans la même perspective[413]. Le groupe *Open WhisperSystems* a développé et offre, quant à lui, les applications *RedPhone*, permettant le cryptage des appels téléphoniques effectués sur un appareil de téléphonie cellulaire, ainsi que *TextSecure*, permettant le cryptage des communications transmises par le

---

[411] Nate CARDOZO, Cindy COHN, Parker HIGGINS, Kurt OPSAHL et Rainey REITMAN, *Who has your back? Protecting Your Data from Government Requests*, Electronic Frontier Foundation, 2014, en ligne : <https://www.eff.org/files/2014/05/19/who-has-your-back-2014-govt-data-requests.pdf> (dernière consultation le 18 février 2015).

[412] Voir le site Internet du *Blackphone*, en ligne : <https://www.blackphone.ch/#introduction> (dernière consultation le 18 février 2015).

[413] Voir le site Internet de *Silent Circle*, en ligne : <https://silentcircle.com/services> (dernière consultation le 18 février 2015).

biais de la messagerie textuelle[414]. De plus, *RetroShare* a développé une plateforme de communication décentralisée au sein de laquelle les utilisateurs peuvent échanger des messages cryptés[415]. Il ne s'agit là que de trois exemples d'entreprises et de regroupements ayant innové afin de placer la vie privée de leurs utilisateurs au cœur de leur démarche commerciale, mais ils illustrent le fait que l'évolution technologique et la protection des droits fondamentaux ne sont pas deux concepts antinomiques[416]. Finalement, l'*Electronic Frontier Foundation* a récemment procédé à l'évaluation de 39 outils ou technologies de communication, en se fondant sur sept critères prédéfinis, dont le cryptage des communications *en transit*, la capacité du fournisseur à prendre connaissance du contenu des messages et à vérifier l'identité des contacts des utilisateurs, ainsi que la possibilité d'évaluer indépendamment le code source de l'application[417].

Il ressort de ce qui précède que les différents acteurs participant à la discussion planétaire entourant la surveillance électronique gouvernementale à grande échelle sont susceptibles d'y apporter des éléments distincts, tous aussi pertinents les uns que les autres.

---

[414] Voir le site Internet de *Open WhisperSystems*, en ligne : <https://whispersystems.org/> (dernière consultation le 18 février 2015).

[415] Voir le site Internet de *RetroShare*, en ligne : <http://retroshare.sourceforge.net/index.html> (dernière consultation le 18 février 2015).

[416] Les travaux du Professeur Lawrence Lessig font, à cet égard, autorité. Ainsi, le Professeur Lessig avance : « [the] code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates ». Voir Lawrence LESSIG, « Code is Law. On Liberty in Cyberspace », *Harvard Magazine* 2000, en ligne : <http://harvardmagazine.com/2000/01/code-is-law-html> (dernière consultation le 18 février 2015). Voir également Ann CAVOUKIAN, *Privacy by Design. Strong Privacy Protection – Now, and Well into the Future*, 2011, en ligne : <http://www.ipc.on.ca/images/Resources/PbDReport.pdf> (dernière consultation le 18 février 2015).

[417] ELECTRONIC FRONTIER FOUNDATION, « Secure Messaging Scorecard » (6 novembre 2014), en ligne : <https://www.eff.org/secure-messaging-scorecard> (dernière consultation le 18 février 2015).

Cela étant, les États sont investis de la capacité d'assurer une protection directe à la vie privée informationnelle de leurs citoyens, par le biais de leur monopole des processus législatif et judiciaire traditionnels. Les ONG apportent, pour leur part, une critique indépendante et objective de la nature et de la portée des activités étatiques de surveillance électronique, en plus, dans bien des situations, de proposer des manières alternatives de réfléchir sur les enjeux soulevés par ces activités. Les entreprises et autres groupes sont, quant à eux, en mesure de concentrer leur expertise technique et d'innover, au bénéfice de la vie privée des utilisateurs de leurs services. Ces éléments, dont nous tenons compte à titre de considérations extrinsèques, contribuent directement, au même titre que les implications sociales de la surveillance électronique des métadonnées[418], à la contextualisation et, ultimement, à l'enrichissement de la réflexion au cœur de ce mémoire.

En conclusion, nous avons démontré, dans cette sous-partie, que l'étude d'une multitude d'éléments ne relevant pas, à proprement parler, de la sphère juridique était susceptible d'approfondir notre réflexion. Il est une chose que d'élaborer un raisonnement purement juridique, aussi solide soit-il, mais il en est une autre que de s'assurer qu'il s'intègre harmonieusement dans la société au sein de laquelle il vise à s'appliquer, conçue comme un tout. Ceci étant, la nature constitutionnelle, donc intrinsèquement politique et sociale, de notre réflexion, de même que l'importance et les particularités inhérentes au concept de vie privée[419], rendent absolument nécessaire la prise en compte de ces éléments non juridiques. Sur ce point, la Cour suprême du Canada a déjà jugé, nous le rappelons, que « [l]'interdiction

[418] *Supra*, 3.2.1.
[419] Sur le caractère fondamentalement complexe de la vie privée, voir *supra*, 1.1.

qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique » et « [que] [n]aturellement, un équilibre doit être établi entre les revendications en matière de vie privée et les autres exigences de la vie en société »[420].

Or, nul ne saurait raisonnablement prétendre que « l'essence même d'un État démocratique », les « revendications en matière de vie privée » et les « exigences de la vie en société » sont des concepts exclusivement juridiques. Le droit constitutionnel a, certes, vocation à régir ceux-ci, mais ils ne sauraient être précisés que suite à l'analyse de leur dimension sociale, politique, culturelle ou encore philosophique. Il en va de la crédibilité de tout raisonnement juridique, particulièrement lorsque les enjeux soulevés sont délicats. C'est ainsi que nous avons décidé d'appréhender notre question de recherche. Le fait d'avoir ciblé, puis de nous être penchés sur quatre implications sociales découlant de la surveillance à grande échelle des métadonnées des communications électroniques, nous a fourni plusieurs indices nous permettant de contextualiser adéquatement la réflexion au cœur de ce mémoire.

Dans la même perspective, nous nous sommes également intéressés à plusieurs considérations extrinsèques. Bien que ne contribuant pas, directement, à l'élaboration, ou encore à l'articulation de notre argumentaire, elles illustrent néanmoins parfaitement le fait que le questionnement qui nous anime s'inscrit dans la discussion, voire la réflexion globale sur la multitude d'enjeux entourant la surveillance électronique à grande échelle des métadonnées.

---

[420] *R.* c. *Dyment*, préc., note 105, 427-428.

Ces considérations nous incitent à conclure qu'il existe, au sein des États occidentaux et sur la scène internationale, d'importantes préoccupations quant à la mise en place et à l'utilisation de dispositifs de surveillance à grande échelle visant spécifiquement le public. Elles soulignent également le besoin criant d'un encadrement et d'une limitation efficace et crédible de ces activités. Nous estimons qu'un tel encadrement passe, au Canada, par une protection constitutionnelle des métadonnées, à travers l'élargissement du cadre d'analyse du « Biographical core », conformément au raisonnement que nous avons exposé dans la sous-partie précédente[421].

Conclusion provisoire

Cette troisième et dernière partie de notre mémoire portait spécifiquement sur l'étendue de la protection constitutionnelle de la vie privée informationnelle dans l'environnement technologique actuel, caractérisé par la surveillance électronique gouvernementale à grande échelle et la collecte des métadonnées des communications électroniques. Cette partie visait, plus particulièrement, à évaluer la capacité du cadre d'analyse du « Biographical core » à assurer une réelle protection à ces métadonnées afin, ultimement, de déterminer s'il était nécessaire d'élaborer une nouvelle conception de la vie privée informationnelle en droit canadien, mieux adaptée à la réalité contemporaine. Pour ce faire, nous nous sommes, dans un premier temps, penchés sur le caractère « biographique d'ordre personnel » des métadonnées des communications électroniques. À la suite de cette analyse, nous avons conclu que les principes constitutionnels pertinents favorisaient assurément un élargissement de la portée du

[421] *Supra*, 3.1.

« Biographical core », spécialement à la lumière des capacités d'analyse que permet leur agrégation, du dépassement juridique total de la distinction contenu-métadonnées puis, finalement, de la nature intrinsèquement privée des renseignements visés par les activités de surveillance gouvernementale. Afin d'appuyer cette conclusion, nous nous sommes intéressés à l'approche favorisée par la Cour suprême quant à l'interprétation de l'article 8 de la *Charte canadienne*. Après ce détour obligé dans la sphère interprétative, il nous semble raisonnable de croire, advenant le cas où le plus haut tribunal du pays se pencherait sur une question similaire à la nôtre, que la portée du « Biographical core » soit élargie, de manière à assurer aux métadonnées des communications électroniques la protection constitutionnelle de l'article 8.

L'étude des implications sociales et des considérations extrinsèques à laquelle nous nous sommes livrés, dans un deuxième temps, conforte cette conclusion. En effet, nous avons rapidement constaté que le positionnement de notre argumentaire constitutionnel est susceptible d'apporter une solution aux enjeux non juridiques soulevés par la surveillance gouvernementale à grande échelle. Nous avons également réalisé, à la suite de l'analyse de plusieurs considérations extrinsèques, que notre réflexion participe, voire s'intègre pleinement à la discussion planétaire entourant ces enjeux. Bien que complémentaire à l'élaboration juridique de notre raisonnement, nous estimons que cette démarche en est absolument indissociable, dans la mesure où elle contribuer à expliquer, contextualiser et justifier notre argumentaire.

Ainsi, nous ne croyons pas qu'il soit nécessaire, au regard de l'ensemble des faits, principes, règles d'interprétation et autres éléments considérés dans ce mémoire, de délaisser le cadre d'analyse du « Biographical core », au bénéfice d'une nouvelle conception de la vie privée informationnelle. Rien ne semble s'opposer à ce que la portée de ce cadre d'analyse soit élargie, à travers une interprétation téléologique et évolutive de l'article 8 de la *Charte canadienne*, et ce, particulièrement à la lumière des éléments étudiés, lesquels y sont, à notre humble avis, définitivement favorables.

Nous en venons à cette conclusion après avoir soupesé, avec tout le sérieux que commande un tel processus, une myriade de facteurs aussi pertinents que diversifiés. Ceci étant, nous avons dû, dans un souci de concision, prioriser ceux qui nous semblaient les plus importants ou encore qui s'intégraient simplement mieux dans notre raisonnement. Il a donc naturellement découlé du choix de notre approche de recherche que nous mettions l'accent sur la portée de la définition constitutionnelle de la vie privée informationnelle. Il aurait toutefois été fort enrichissant de nous intéresser à d'autres considérations tout aussi fondamentales à l'appréhension des enjeux soulevés par les activités gouvernementales de surveillance électronique à grande échelle. Nous aurions, par exemple, pu approfondir la question de la place qu'occupent ces activités au sein de toute société libérale digne de ce nom, de même que les risques qu'elles soulèvent pour leur caractère démocratique[422]. Il nous aurait également été

---

[422] Certains pourraient avancer que des activités de surveillance d'une telle ampleur semblent irréconciliables avec le concept même de démocratie libérale occidentale. À ce sujet, les propos de la Cour suprême, sous la plume du juge La Forest, dans l'arrêt *R.* c. *Wong*, préc., note 178, sont instructifs : « [j]'estime fermement que si une société libre et ouverte ne peut tolérer la possibilité qu'en l'absence d'autorisation judiciaire, les agents de l'État aient le droit d'enregistrer les propos de qui ils veulent, il est également inconcevable que l'État ait le pouvoir discrétionnaire illimité de soumettre qui il veut à une surveillance magnétoscopique effectuée subrepticement. […] La notion selon laquelle les agents de l'État devraient être libres de braquer des caméras

possible d'analyser notre question de recherche sous l'angle de la justification des activités de surveillance de cette nature, en vertu de l'examen prévu à l'article premier de la *Charte canadienne*[423].

Bref, nous sommes conscients du fait que le cadre d'analyse du « Biographical core » ne fasse pas l'unanimité dans la doctrine juridique canadienne[424]. Néanmoins, d'aucuns ne sauraient prétendre, face à la gravité de la problématique à laquelle la surveillance électronique à grande échelle des métadonnées des communications électroniques nous confronte, tant sur les plans juridique, social et politique, que le statu quo est acceptable. Conséquemment, il est inconcevable, dans un État de droit comme le Canada, que le gouvernement soit autorisé à recueillir, à sa discrétion et sans aucune forme de contrôle judiciaire préalable, une quantité virtuellement illimitée de renseignements personnels sur la quasi totalité des individus présents sur son territoire. Ce faisant, nous demeurons convaincus qu'une protection plus adéquate de la vie privée informationnelle doit, aujourd'hui, impérativement découler d'un élargissement de la portée du cadre d'analyse du « Biographical

---

dissimulées sur des membres de la société, en tout temps et en tout lieu, à leur gré, est fondamentalement irréconciliable avec notre perception d'un comportement acceptable de la part des gouvernements » (p. 47).

[423] À ce sujet, il nous semblerait, à première vue, très surprenant, que les tribunaux – malgré toute la déférence dont ils font preuve à l'égard des décisions gouvernementales en matière de sécurité nationale – jugent qu'une règle de droit autorisant la surveillance à grande échelle et la collecte systématique des métadonnées des communications électroniques porte atteinte au droit garanti à l'article 8 « dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique », au sens de l'article premier. Pour plus de détails sur ce processus, voir l'arrêt *R.* c. *Oakes*, préc., note 325.

[424] Renee M. Pomerance considère, par exemple, que le « Biographical core » n'est pas apte à assurer une pleine protection à la vie privée informationnelle, face à l'émergence de nouvelles technologies toujours plus invasives et qu'une redéfinition du droit à la vie privée s'impose. Voir Renee M. POMERANCE, « Redefining Privacy in the Face of New Technologies : Data Mining and the Threat to the ''Inviolate Personality'' », (2005) 9 *Can. Crim. L. Rev.* 273. Voir également Lisa M. AUSTIN, « Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter », (2007) 57 *U.T.L.J* 499, ainsi que Stuart HARGREAVES, « *R. v. Gomboc*: Considering the Proper Role of the "Biographical Core" in a Section 8 Informational Privacy Analysis », (2013) 59 *C.L.Q.* 86, 103-106.

core ». Nous estimons avoir démontré, à la lumière de l'ensemble des circonstances pertinentes, que cette position est tout à fait justifiable et parfaitement raisonnable.

CONCLUSION

> *L'un des effets les plus destructeurs du terrorisme, c'est sa capacité de provoquer des réactions qui sapent les valeurs démocratiques fondamentales sur lesquelles sont fondés nos pays démocratiques. La crainte et la colère suscitées par le terrorisme peuvent amener des dirigeants à faire la guerre à des cibles qui ne sont pas nécessairement liées à l'incident terroriste lui même. Ou encore, elles peuvent conduire des gouvernements à restreindre les libertés civiles et à recourir à des tactiques, telle la torture, qu'ils dénonceraient normalement — tactiques qui, avec le recul, ne s'avéreront peut-être pas nécessaires ou justifiables.*
>
> La très honorable Beverley McLachlin, C.P., juge en chef du Canada[425]

La réflexion proposée dans ce mémoire avait essentiellement pour objet de démontrer que la portée de l'article 8 de la *Charte canadienne* était susceptible d'être élargie, d'une manière qui soit plus représentative de la prégnance des nouvelles technologies de l'information et des communications dans la société canadienne. Plus spécifiquement, notre démarche intellectuelle visait à mettre de l'avant, explorer, puis appuyer la position selon laquelle rien ne s'oppose à ce que le cadre d'analyse du « Biographical core », qui détermine l'étendue de la protection constitutionnelle dévolue à la vie privée informationnelle en droit canadien, soit en mesure de s'appliquer aux métadonnées des communications électroniques, dans le contexte de leur surveillance à grande échelle par les autorités gouvernementales.

Pour ce faire, nous avons consacré la première partie de ce mémoire à la démonstration selon laquelle la vie privée revêt une importance considérable dans la vie des individus, aussi bien que dû aux fonctions essentielles dont elle rend possible l'exercice, sur le plan collectif. Nous avons donc, dans un premier temps, insisté sur le rôle que joue l'aménagement et la

---

[425] B. MCLACHLIN, préc., note 387.

préservation d'une sphère privée dans le développement d'une quelconque individualité, lequel repose inévitablement sur un processus d'élaboration des idées et d'expérimentation intime[426]. Nous avons également souligné le fait que l'individualité mène à l'autonomie morale, laquelle, à son tour, contribue directement à la participation efficace et pertinente des citoyens aux processus sociaux et politiques chers à notre conception de la démocratie canadienne[427].

Nous avons, par la suite, établi que les métadonnées des communications électroniques avaient, au XXI^{e} siècle, le potentiel de révéler des renseignements potentiellement personnels, donc de nature privée, sur les individus[428]. Ce constat nous a forcé à conclure, à la suite de l'étude de certaines activités de gouvernementales menées à des fins de sécurité nationale, à commencer par la surveillance électronique et la collecte à grande échelle des métadonnées des communications électroniques, que celles-ci étaient aptes à entraver sérieusement la protection de la vie privée dont jouissent les Canadiens[429]. La gravité de l'atteinte résultant de telles activités découle, en grande partie, de la confusion technique existant désormais entre le contenu des communications électroniques et les métadonnées y étant associées. Par ailleurs, même en l'absence d'une telle confusion, les métadonnées sont susceptibles de révéler, à leur face même, un éventail d'éléments privés, et ce, particulièrement à la lumière du raffinement des méthodes de collecte et d'analyse à la disposition des autorités gouvernementales.

---

[426] *Supra*, 1.1.1.
[427] *Supra*, 1.1.2.
[428] *Supra*, 1.2.1.
[429] *Supra*, 1.2.2.

Nous avons ensuite présenté, dans la deuxième partie de ce mémoire, l'étendue de la protection normative accordée, en droit canadien, à la vie privée. Nous avons constaté, d'un point de vue constitutionnel général, que l'article 7 de la *Charte canadienne* protégeait indirectement la vie privée, à travers la portée jurisprudentielle conférée aux droits à la liberté ainsi qu'à la sécurité[430]. Nous avons toutefois insisté sur la démonstration du fait que la part du lion de la protection constitutionnelle de la vie privée reposait sur l'article 8 de la *Charte canadienne*, qui prévoit le droit à une protection contre les fouilles, les perquisitions ou les saisies abusives[431].

Nous avons alors pu nous concentrer, dans une perspective plus spécifique à notre réflexion, sur la protection constitutionnelle de la vie privée informationnelle[432]. Nous avons établi que la teneur et l'étendue de la protection de cette dimension de la vie privée étaient déterminées par le cadre d'analyse du « Biographical core ». Ce cadre d'analyse limite la protection de l'article 8 de la *Charte canadienne* aux seuls renseignements présentant un caractère biographique d'ordre personnel et étant susceptibles de révéler des détails intimes sur les choix et le mode de vie d'un individu. Or, il s'est révélé qu'une certaine incertitude semblait caractériser la capacité du « Biographical core » à protéger, dans certains cas de figure, la vie privée informationnelle, notamment due aux difficultés inhérentes à la détermination précise de l'objet d'une fouille, perquisition ou saisie en matière informationnelle, de même qu'à celles découlant de l'existence et de la portée, dans une situation donnée, d'une quelconque protection constitutionnelle.

---

[430] *Supra*, 2.1.1.1.
[431] *Supra*, 2.1.1.2.
[432] *Supra*, 2.2.

Finalement, à la lumière de l'importance de la vie privée, du grave danger que présentent, pour les droits fondamentaux et la démocratie, certaines activités de surveillance gouvernementale, ainsi que de la complexité de la détermination exacte de la teneur de la protection constitutionnelle de la vie privée informationnelle, il nous est apparu nécessaire de consacrer la troisième et dernière partie de ce mémoire au cœur de notre réflexion. Plus spécifiquement, nous nous sommes penchés sur la capacité du cadre d'analyse du « Biographical core » à protéger adéquatement les métadonnées des communications électroniques au regard des activités gouvernementales visant leur surveillance électronique et leur collecte à grande échelle.

Pour ce faire, nous avons d'abord développé un argumentaire selon lequel les métadonnées des communications électroniques présentaient un caractère intrinsèquement biographique et personnel, lequel se trouve aujourd'hui dramatiquement accentué par la nature et la portée des activités de surveillance gouvernementale[433]. Nous avons ensuite démontré que les principes gouvernant l'interprétation de l'article 8 de la *Charte canadienne* nous permettaient de conclure, particulièrement dans le contexte des nouvelles technologies de l'information et des communications et conformément à notre angle de recherche, à la possibilité d'un élargissement de la portée du cadre d'analyse du « Biographical core », de manière à y inclure les métadonnées des communications électroniques[434]. Nous avons finalement renforcé notre argumentaire en le resituant par rapport à un ensemble de considérations non juridiques, mais cruciales à la conceptualisation de notre réflexion, à savoir

[433] *Supra*, 3.1.1.
[434] *Supra*, 3.1.2.

les implications sociales soulevées par la surveillance électronique des métadonnées[435] et le contexte mondial au sein duquel les enjeux impliqués par cette question sont appréhendés[436].

Il nous apparaît désormais opportun de répondre explicitement à la question que nous nous sommes posée dès le commencement de ce mémoire :

> Le cadre d'analyse du « Biographical core », qui conditionne la portée de la protection accordée à la vie privée informationnelle en vertu de l'article 8 de la *Charte canadienne des droits et libertés*, est-il susceptible d'inclure les métadonnées des communications électroniques?

Nous sommes convaincus, à la suite d'une réflexion sérieuse, posée et objective, ainsi qu'à l'étude de l'ensemble des éléments présentés dans ce mémoire, que cette question doit recevoir une réponse affirmative. L'interprétation des conclusions qu'il est raisonnablement possible d'inférer, à la suite de l'analyse élaborée dans ce mémoire, nous indique donc que le cadre d'analyse du « Biographical core » est susceptible d'être élargi, de manière à assurer une certaine protection constitutionnelle aux métadonnées des communications électroniques, dans le contexte de leur surveillance électronique et leur collecte à grande échelle par les autorités gouvernementales. Ainsi, nous estimons avoir ouvert la voie, à travers notre démarche de recherche, à l'élaboration et à l'articulation d'une protection constitutionnelle spécifique des métadonnées des communications électroniques. Néanmoins, il n'était pas dans notre objectif de nous pencher sur les modalités concrètes que pourrait être appelée à prendre cette protection.

---

[435] *Supra*, 3.2.1.
[436] *Supra*, 3.2.2.

Dans une perspective complémentaire, nous sommes conscients que l'approche constitutionnelle, qui commande un recours aux tribunaux, ne nous paraît pas en mesure – aussi appropriée soit-elle dans le cas de figure qui nous intéresse – de trancher de manière décisive et optimale l'éternel débat entourant la limitation du pouvoir de surveillance de l'État et la préservation des droits et libertés fondamentaux. Dû à son infinie complexité, la solution, s'il en existe une, repose selon nous dans les mains du législateur, pour la simple et unique raison qu'il semble mieux outillé que les tribunaux pour réguler l'utilisation, par les autorités gouvernementales, de technologies de surveillance en constante évolution[437]. L'opportunité de légiférer ne s'avère toutefois pas garante d'un quelconque accroissement de la protection accordée à la vie privée, particulièrement en matière de surveillance de sécurité, et ce, d'autant plus dans le contexte actuel. Claude Fabien écrivait d'ailleurs, en 1970, que :

> L'opportunité d'une intervention législative s'apprécie à la lumière de deux facteurs principaux : d'une part, l'existence objective du problème et son degré d'urgence, et d'autre part la volonté de l'électorat de voir le problème se régler. Ce dernier facteur soulève la question de la rentabilité politique de l'intervention. Cette volonté de l'électorat est généralement conditionnée par la connaissance que les citoyens ont du problème et ensuite par le prix qu'ils sont prêts à payer pour le résoudre.[438]

Or, il appert aujourd'hui manifestement que la question de notre « vulnérabilité » collective, face à la menace diffuse que présentent les groupes terroristes de toutes sortes, de même que la nécessité corrélative de s'en protéger, semble considérablement plus pressante que celle de préserver l'intégrité de la protection constitutionnelle garantie au droit à la vie privée de tout un chacun. Tant et aussi longtemps que la préservation de la sécurité et la

---

[437] Steven Penney affirme à ce propos que: « [l]egislatures are generally better equipped than courts to regulate the use of novel and evolving surveillance technologies ». Voir S. PENNEY, préc., note 163, par. 33.

[438] Claude FABIEN, *Ordinateur et vie privée : techniques et contrôle. Rapport au groupe d'étude sur l'ordinateur et la vie privée*, Ottawa, Information Canada, 1970, p. 3.

protection de la vie privée seront perçues comme étant mutuellement exclusives ou, à tout le moins, comme étant des valeurs opposées au sein d'un exercice de pondération, nous entretenons bien peu d'espoir face à un quelconque changement d'attitude législative.

Notre position face aux questions abordées dans ce mémoire ne nous empêche toutefois pas de reconnaître le caractère fondamental des activités gouvernementales de surveillance à des fins de sécurité nationale, y compris celles visant les métadonnées des communications électroniques. Néanmoins, ces activités deviennent discutables, voire problématiques, en démocratie, à partir du moment où il est établi qu'elles ne visent plus seulement certains individus précis, mais bien tout le monde, en tout temps. À cet égard, les propos du juge La Forest concernant la surveillance électronique gouvernementale, dans l'arrêt *R.* c. *Duarte*, sont particulièrement éloquents – et d'actualité :

> [La] [réglementation du pouvoir de l'État d'enregistrer des communications dont l'auteur s'attend à ce qu'elles ne soient entendues que par leur destinataire] s'explique par la conscience du fait que, si l'État était libre de faire, à son entière discrétion, des enregistrements électroniques permanents de nos communications privées, il ne nous resterait rien qui vaille de notre droit de vivre libre de toute surveillance. La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications restent privées. Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens. […] S'il est permis à l'État d'enregistrer et de transmettre arbitrairement nos communications privées, il devient dès lors impossible de trouver un juste équilibre entre le droit du particulier d'être laissé tranquille et le droit de l'État de porter atteinte à la vie privée dans la poursuite de ses objets, notamment la nécessité d'enquêter sur le crime et de le combattre.
>
> Ce n'est pas nier qu'il est d'importance vitale pour les organismes chargés de l'application des lois d'être en mesure de recourir à la surveillance électronique dans leurs enquêtes sur le crime. La surveillance électronique joue un rôle indispensable dans la découverte d'opérations criminelles complexes. Son utilité

> dans les enquêtes en matière de stupéfiants, par exemple, a été maintes fois confirmée. Mais, pour les raisons déjà évoquées, il est inadmissible dans une société libre que les organes de l'État puissent se servir de cette technologie à leur seule discrétion. Le péril pour la vie privée serait tout à fait inacceptable.[439] (nos soulignements)

En plus des risques manifestes qu'elles présentent, les activités de surveillance à grande échelle sont affligées d'un déficit de légitimité considérable, au regard des principes démocratiques que leur mise en place vise, en tout premier lieu, à protéger. Qui plus est, il nous semble inapproprié d'aborder la sécurité nationale dans une perspective de prévention, à n'importe quel prix, des attentats ou attaques terroristes. Le jeu démocratique occidental nous impose d'intégrer à cette mission de prévention, par ailleurs absolument cruciale, l'objectif tout aussi important de préservation des principes constitutionnels inhérents à la nature même de l'organisation de notre société. En d'autres termes, toute mesure de lutte au terrorisme ayant vocation à être appliquée en territoire canadien, y compris la surveillance à grande échelle des métadonnées des communications électroniques, doit nécessairement tenir compte des impératifs constitutionnels, politiques et sociaux caractéristiques de la société canadienne, à commencer par la protection de la vie privée.

La mise en place, à l'échelle de l'ensemble de la société, de mesures permettant de garantir l'absence absolue de tout risque, quel qu'il soit, en matière de sécurité nationale, impliquerait, au bas mot, une remise en question de son caractère démocratique. Ses citoyens seraient, à cet égard, aussi vulnérables au vent de la tyrannie et de l'oppression que le serait, face au souffle glacial de l'hiver, celui qui, pour se débarrasser de la vermine qu'il croit avoir entendu y rôder, met feu à son habitation. Nous n'en sommes, bien entendu, pas là, mais c'est

---

[439] *R.* c. *Duarte*, préc., note 221, 44-45.

dans cet esprit que nous avons mené la réflexion présentée dans ce mémoire et que nous estimons que la protection constitutionnelle des métadonnées des communications électroniques s'avère aujourd'hui cruciale.

Bref, peut-être un important recul s'impose-t-il afin d'être en mesure d'évaluer adéquatement et avec lucidité les tensions au cœur même de cette « guerre » au terrorisme, entamée il y a déjà près d'une quinzaine d'années et dont le sujet du présent mémoire constitue un vibrant exemple? Peut-être ces tensions seront-elles inévitables tant et aussi longtemps que cette « guerre » n'aura pas été « gagnée », pour autant que nous soyons, collectivement, en position de le réaliser? Autrement, un état tel état de « guerre » rend-il logiquement impossible toute coexistence durable entre notre besoin de sécurité et notre désir de liberté? Le révolutionnaire James Madison, l'un des « Founding Fathers » des États-Unis, écrivit, à ce propos, il y a désormais 220 ans :

> Of all the enemies to public liberty war is, perhaps, the most to be dreaded, because it comprises and develops the germ of every other. […] No nation could preserve its freedom in the midst of continual warfare.[440]

Nous laisserons à d'autres le soin de méditer sur ces questions. Quoi qu'il en soit, c'est avec passion que nous espérons avoir pu effleurer certains des enjeux qui s'annoncent cruciaux pour le XXI^{e} siècle et, bien humblement, avoir su poser une pierre, aussi modeste soit-elle, sur l'édifice du savoir juridique. La réflexion se poursuit.

Me Alexandre Thibeault
Mars 2015

---

[440] Scott HORTON, « Madison on the Dangers of War », *Harper's Magazine* (7 juillet 2007), en ligne : <http://harpers.org/blog/2007/07/madison-on-the-dangers-of-war/> (dernière consultation le 18 février 2015).

BIBLIOGRAPHIE

Législation

Canada

Lois à caractère constitutionnel et quasi-constitutionnel

Charte canadienne des droits et libertés, Partie 1 de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.).

Charte des droits et libertés de la personne, L.R.Q., c. C-12.

Déclaration canadienne des droits, L.C. 1960, c. 4.

Codes

Code civil du Québec, L.Q. 1991, c. 64.

Code criminel, L.R.C. 1985, c. C-46.

Lois

Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-1.1.

Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20.

Access to Information and Protection of Privacy Act, S.N.W.T. (Nu.) 1994, c. 20.

Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1.

Freedom of Information and Protection of Privacy Act, C.C.S.M., c. F175.

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.

Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.

Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 1988, c. F-15.01.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31.

Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5.

Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01.

Health Information Act, R.S.A. 2000, c. H-5.

Health Information Protection Act, S.S. 1999, c. H-0.021.

Loi antiterroriste, L.C. 2001, c. 41.

Loi canadienne sur les droits de la personne, L.R.C. 1985, c. H-6.

Loi relative aux enquêtes sur les coalitions, L.R.C. 1985, c. 19 (2e supp.).

Loi sur l'accès à l'information, L.R.C. 1985, c. A-1.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1.

Loi sur la défense nationale, L.R.C. 1985, c. N-5.

Loi sur la Gendarmerie royale du Canada, L.R.C. 1985, c. R-10.

Loi sur la protection de la vie privée, L.C. 1973-74, c. 50.

Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21.

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5.

Loi sur le ministère de la Sécurité publique et de la Protection civile, L.C. 2005, c. 10.

Loi sur le Service canadien du renseignement de sécurité, L.R.C. 1985, c. C-23.

Personal Health Information Access and Protection of Privacy Act, S.B.C. 2008, c. 38.

Personal Health Information Act, C.C.S.M., c. P33.5.

Personal Health Information Act, S.N.L. 2008, c. P-7.01.

Personal Health Information Act, S.N.S. 2010, c. 41.

Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05.

Personal Health Information Protection Act, S.O. 2004, c. 3, Sch. A.

Personal Information Protection Act, S.A. 2003, c. P-6.5.

Personal Information Protection Act, S.B.C. 2003, c. 63.

Privacy Act, L.R.C. 1985, c. P-21.

Privacy Act, R.S.B.C. 1996, c. 373.

Privacy Act, R.S.M. 1987, c. P-125.

Privacy Act, R.S.N.L. 1990, c. P-22.

Privacy Act, R.S.S. 1978, c. P-24.

Right to Information and Protection of Privacy Act, S.N.B. 2009, c. R-10.6.

États-Unis

Lois à caractère constitutionnel et quasi-constitutionnel

United States Bill of Rights, U.S. Const., amend. I-X.

Lois

Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C., § 3711.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

Jurisprudence

Canada

B. (R.) c. *Children's Aid Society of Metropolitan Toronto*, [1995] 1 R.C.S. 315.

Blencoe c. *Colombie-Britannique (Human Rights Commission)*, [2000] 2 R.C.S. 307.

British Columbia Securities Commission c. *Branch*, [1995] 2 R.C.S. 3.

Godbout c. *Longueuil (Ville)*, [1997] 3 R.C.S. 844.

Gosselin c. *Québec (Procureur général)*, [2002] 4 R.C.S. 429.

Hill c. *Église de scientologie de Toronto*, [1995] 2 R.C.S. 1130.

Hunter c. *Southam Inc.*, [1984] 2 R.C.S. 145.

McInerney c. *MacDonald*, [1992] 2 R.C.S. 138.

Mills c. *La Reine*, [1986] 1 R.C.S. 863.

Nouveau Brunswick (Ministre de la Santé et des Services communautaires) c. *G. (J.)*, [1999] 3 R.C.S. 46.

R. c. *A.M.*, [2008] 1 R.C.S. 569.

R. c. *Beare*, [1988] 2 R.C.S. 387.

R. c. *Big M Drug Mart Ltd.*, [1985] 1 R.C.S. 295.

R. c. *Buhay*, [2003] 1 R.C.S. 631.

R. c. *Caslake*, [1998] 1 R.C.S. 51.

R. c. *Clay*, [2003] 3 R.C.S. 735.

R. c. *Colarusso*, [1994] 1 R.C.S. 20.

R. c. *Cole*, [2012] 3 R.C.S. 34.

R. c. *Collins*, [1987] 1 R.C.S. 265.

R. c. *Duarte*, [1990] 1 R.C.S. 30.

R. c. *Dyment*, [1988] 2 R.C.S. 417.

R. c. *Edwards*, [1996] 1 R.C.S. 128.

R. c. *Evans*, [1996] 1 R.C.S. 8.

R. c *Fearon*, 2014 CSC 77.

R. c. *Feeney*, [1997] 2 R.C.S. 13.

R. c. *Genest*, [1989] 1 R.C.S. 59.

R. c. *Godoy*, [1999] 1 R.C.S. 311.

R. c. *Gomboc*, [2010] 3 R.C.S. 211.

R. c. *Grant*, [2009] 2 R.C.S. 353.

R. c. *Kokesch*, [1990] 3 R.C.S. 3.

R. c. *Law*, [2002] 1 R.C.S. 227.

R. c. *M. (M.R.)*, [1998] 3 R.C.S. 393.

R. c. *MacDonald*, [2014] CSC 3.

R. c. *Malmo-Levine; R.* c. *Caine*, [2003] 3 R.C.S. 571.

R. c. *Mills*, [1999] 3 R.C.S. 668.

R. c. *Morelli*, [2010] 1 R.C.S. 253.

R. c. *Morgentaler*, [1988] 1 R.C.S. 30.

R. c. *Oakes*, [1986] 1 R.C.S. 103.

R. c. *O'Connor*, [1995] 4 R.C.S. 411.

R. c. *Patrick*, [2009] 1 R.C.S. 579.

R. c. *Plant*, [1993] 3 R.C.S. 281.

R. c. *Pohoretsky*, [1987] 1 R.C.S. 945.

R. c. *Shoker*, [2006] 2 R.C.S. 399.

R. c. *Silveira*, [1995] 2 R.C.S. 297.

R. c. *Société TELUS Communications*, [2013] 2 R.C.S. 3.

R. c. *Stillman*, [1997] 1 R.C.S. 607.

R. c. *Tessling*, [2004] 3 R.C.S. 432.

R. v. *Trapp*, [2011] SKCA 143.

R. c. *Vu*, [2013] 3 R.C.S. 657.

R. v. *Ward*, [2012] ONCA 660.

R. c. *Wise*, [1992] 1 R.C.S. 527.

R. c. *Wong*, [1990] 3 R.C.S. 36.

R. c. *Spencer*, [2014] CSC 43.

Renvoi sur la Motor Vehicle Act (C.-B.), [1985] 2 R.C.S. 486.

Rodriguez c. *Colombie Britannique (Procureur général)*, [1993] 3 R.C.S. 519.

Schreiber c. *Canada (Procureur général)*, [1998] 1 R.C.S. 841.

Siemens c. *Manitoba (Procureur général)*, [2003] 1 R.C.S. 6.

Singh c. *Ministre de l'Emploi et de l'Immigration*, [1985] 1 R.C.S. 177.

Suresh c. *Canada (Ministre de la Citoyenneté et de l'Immigration*, [2002] 1 R.C.S. 3.

Thomson Newspapers Ltd. c. *Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425.

États-Unis

Katz v. *United States*, [1967] 389 U.S. 347.

Olmstead v. *United States*, [1928] 277 U.S. 438.

Riley v. *California*, [2014] 573 U.S. ___.

United States v. *Miller*, [1976] 425 U.S. 435.

Doctrine

Monographies

ALLEN, Anita L., *Uneasy Access. Privacy for Women in a Free Society*, Totowa, Rowman & Littlefield, 1988.

ARENDT, Hannah, *Condition de l'homme moderne*, coll. Agora, n°24, Paris, Calmann-Lévy, 1988.

BEAULAC, Stéphane, *Précis d'interprétation législative. Méthodologie générale, Charte canadienne et droit international*, Montréal, LexisNexis, 2008.

BENYEKHLEF, Karim, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation*, Montréal, Thémis, 2008.

BENYEKHLEF, Karim et Esther MITJANS (dir.), *Circulation internationale de l'information et sécurité*, Montréal, Thémis, 2012.

BOUCHER, Suzanne et Kenneth LANDA, *Understanding Section 8 : Search, Seizure, and the Canadian Constitution*, Toronto, Irwin Law, 2005.

BRUN, Henri, Guy TREMBLAY et Eugénie BROUILLET, *Droit constitutionnel*, 5e éd., Cowansville, Yvon Blais, 2008.

———, *Droit constitutionnel*, 6e éd., Cowansville, Yvon Blais, 2014.

CARR, James G., *The Law of Electronic Surveillance*, New York, Clark Boardman Company, 1977.

DANDEKER, Christopher, *Surveillance, Power and Modernity. Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge, Polity Press, 1990.

DONOHUE, Laura. K., *The Cost of Counterterrorism. Power, Politics and Liberty*, Cambridge, Cambridge University Press, 2008.

FABIEN, Claude, *Ordinateur et vie privée : techniques et contrôle. Rapport au groupe d'étude sur l'ordinateur et la vie privée*, Ottawa, Information Canada, 1970.

GREENWALD, Glenn, *Nulle part où se cacher*, Paris, JC Lattès, 2014.

HOGG, Peter, *Constitutional Law of Canada*, 5e éd., vol. 2, Toronto, Carswell, 2007.

LANE, Julia, Victoria STODDEN, Stefan BENDER et Helen NISSENBAUM, *Privacy, Big Data, and the Public Good. Frameworks for Engagement*, Cambridge, Cambridge University Press, 2014.

LINDEN, Allen M. et Bruce FELDTHUSEN, *Canadian Tort Law*, 9e éd., Markham, LexisNexis, 2011.

LYON, David, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis, University of Minnesota Press, 1994.

———, *Surveillance Studies. An Overview*, Cambridge, Polity Press, 2007.

MATTELART, Armand, *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, La Découverte, 2007.

MAYER-SCHÖNBERGER, Viktor. et Kenneth CUKIER, *Big Data. A Revolution That Will Transform How We Live, Work and Think*, Londres, John Murray, 2013.

MCISAAC, Barbara, Rick SHIELDS et Kris KLEIN, *The Law of Privacy in Canada*, Carswell, vol. 1, Toronto, 2000.

NAGEL, Thomas, *Concealment and Exposure. And Other Essays*, Oxford, Oxford University Press, 2002.

OSBORNE, Philip H., *The Law of Torts*, 4e éd., Toronto, Irwin Law, 2011.

PIEKALKIEWICZ, Janusz, *World History of Espionage : Agents, Systems, Operations*, Munich, Südwest Verlag, 1988.

POWER, Michael, *Access to Information and Privacy*, 1re éd., coll. « Halsbury's Law of Canada », Markham, LexisNexis, 2011.

———, *Halsbury's Law of Canada. Access to Information and Privacy*, Markham, LexisNexis, 2011.

———, *The Law of Privacy*, Markham, LexisNexis, 2013.

SLOAN, Elinor C., *Security and Defence in the Terrorist Era*, 2e éd., Montréal, McGill-Queen's University Press, 2010.

WATT, David, *Law of Electronic Surveillance in Canada*, Toronto, Carswell, 1979.

WESTIN, Alan F., *Privacy and Freedom*, New York, Atheneum, 1967.

Chapitres de livres et d'ouvrages collectifs

BRUNO, Fernanda, « Surveillance and participation on Web 2.0 », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 343.

CAMPBELL, Duncan, « Inside Echelon : The History, Structure, and Function of the Global Surveillance System Known as Echelon », dans Thomas Y. LEVIN, Ursula FROHNE et Peter WEIBEL (dir.), *CTRL [Space]. Rhetorics of Surveillance from Bentham to Big Brother*, Cambridge, The MIT Press, 2002, p. 158.

DECEW, Judith, « Privacy », dans The Stanford Encyclopedia of Philosophy, Fall 2013 Edition, Stanford, Center for the Study of Language and Information, en ligne : <http://plato.stanford.edu/entries/privacy/>.

EAGLE, Nathan, Alex PENTLAND et David LAZER, « Mobile Phone Data for Inferring Social Network Structure », dans Huan LIU, John J. SALERNO et Michael J. YOUNG (dir.), *Social Computing, Behavioral Modeling, and Prediction*, New York, Springer, 2008, p. 79.

FALK, Richard, « Encroaching on the Rule of Law. Post-9/11 Policies within the United States », dans Alison BRYSK et Gershon SHAFIR (dir.), *National Insecurity and Human Rights. Democracies Debate Counterterrorism*, Berkeley, University of California Press, 2007, p. 14.

MONAHAM, Torin, « Surveillance and terrorism », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge handbook of surveillance studies*, New York, Routledge, 2012, p. 285.

PRIDMORE, Jason, « Consumer surveillance. Context, perspectives and concerns in the personal information economy », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 321.

RACHELS, James, « Why privacy is important », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 290.

SCHAFER, Arthur, « Privacy: A Philosophical Overview », dans Dale GIBSON (dir.), *Aspects of Privacy Law*, Toronto, Butterworths, 1980, p. 1.

SCHOEMAN, Ferdinand D., « Privacy and intimate information », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 403.

STRONG, Tracy B., « self and politics », dans *Encyclopedia of Democratic Thought*, 641, Londres, Routledge.

TUROW, Joseph, « Cracking the Consumer Code : Advertisers, Anxiety, and Surveillance in the Digital Age », dans Kevin D. HAGGERTY et Richard V. ERICSON (dir.), *The New Politics of Surveillance and Visibility*, Toronto, University of Toronto Press, 2006, p. 279.

VAUCLAIR, Martin, « Fouilles et perquisitions: en saisir l'ampleur », dans S.F.P.B.Q*., Congrès annuel du Barreau du Québec (2003)*, Cowansville, Yvon Blais, 2003, p. 27.

WELLER, Toni, « The information state. An historical perspective on surveillance », dans Kristie BALL, Kevin D. HAGGERTY et David LYON (dir.), *Routledge Handbook of Surveillance Studies*, New York, Routledge, 2012, p. 57.

WESTIN, Alan, « The origins of modern claims to privacy », dans Ferdinand D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy. An Anthology*, Cambridge, Cambridge University Press, 1984, p. 56.

Articles de périodiques

AUSTIN, Lisa M., « Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter », (2007) 57 *U.T.L.J* 499.

COHEN, Julie E., « What Privacy is For », (2013) 126-7 *Harv. L. Rev.* 1904.

———, « Examined Lives: Informational Privacy and the Subject as Object », 52-5 *S.L.R.* 1373.

COHEN, Stanley A., « Invasion of Privacy : Police and Electronic Surveillance in Canada », (1982) 27-4 *R.D. McGill* 619.

CORNFIELD, David A., « The Right to Privacy in Canada », (1967) 25 *U.T. Fac. L. Rev.* 103.

COSMAN, Robert W., « A Man's House is his Castle – ''Beep'' : A Civil Law Remedy for the Invasion of Privacy », (1971) 29 *U.T. Fac. L. Rev.* 3.

DAVIES, Alysia, « Invading the Mind : The Right to Privacy and the Definition of Terrorism in Canada », (2006) 3-1 *R.D.T.U.O.* 249.

EAGLE, Nathan et Alex PENTLAND, « Reality mining : sensing complex social systems », (2006) 10-4 *Personal and Ubiquitous Computing* 255.

FORESTER, Nathan, « Electronic Surveillance, Criminal Investigations, and the Erosion of Constitutional Rights in Canada: Regressive U-Turn or a Mere Bump in the Road Towards Charter Justice? », (2010) 73 *Sask. L. Rev.* 23.

FRIED, Charles, « Privacy », (1968) 77-3 *Yale L. J.* 475.

GAVISON, Ruth, « Privacy and the Limits of Law », (1980) 89-3 *Yale L. J.* 421.

GENEST, Alexandre, « Privacy as Construed During the Tessling Era: Revisiting the "Totality of Circumstances Test", Standing and Third Party Rights », (2007) 41 *R.J.T.* 337.

GOLDIE, Janis L., « Virtual Communities and the Social Dimension of Privacy », (2006) 3-1 *R.D.T.U.O.* 133.

HARGREAVES, Stuart, « *R. v. Gomboc*: Considering the Proper Role of the "Biographical Core" in a Section 8 Informational Privacy Analysis », (2013) 59 *C.L.Q.* 86.

HILBERT, Martin et Priscila LÓPEZ, « The World's Technological Capacity to Store, Communicate, and Compute Information », (2011) 332 *Science* 60.

JOCHELSON, Richard, « Trashcans and Constitutional Custodians : The Liminal Spaces of Privacy in the Wake of Patrick », (2009) 72 *Sask. L. Rev.* 199.

LAI, Derek, « Public Video Surveillance by the State : Policy, Privacy Legislation, and the Charter », (2007) 45-1 *Alta. L. Rev.* 43.

LESSIG, Lawrence, « Code is Law. On Liberty in Cyberspace », *Harvard Magazine* 2000, en ligne : <http://harvardmagazine.com/2000/01/code-is-law-html>.

MICHAELSON, Croft, « The Limits of Privacy : Some Reflections on Section 8 of the Charter », (2008) 40-2 *S.C.L.R.* 87.

MONTJOYE, Yves-Alexandre de, César A. HIDALGO, Michel VERLEYSEN et Vincent D. BLONDEL, « Unique in the Crowd : The privacy bounds of human mobility », (2013) 3-1376 *Scientific Reports* 1.

MORGAN, Erin, « Surveillance and Privacy in the 21st Century : The Impact of Bills C-51 (*IP21C*) and C-52 (*IPCEC*) », (2010) 43 *U.B.C. L. Rev.* 471.

PENNEY, Steven, « Unreasonable Search and Seizure and Section 8 of the Charter: Cost-benefit Analysis in Constitutional Interpretation », (2013) 62-2 *S.C.L.R.* 101.

POMERANCE, Renee M., « Redefining Privacy in the Face of New Technologies : Data Mining and the Threat to the ''Inviolate Personality'' », (2005) 9 *Can. Crim. L. Rev.* 273.

PROSSER, William L., « Privacy », (1960) 48-3 *Cal. L. Rev.* 383.

REGAN, Priscilla M., « Privacy as a Common Good in the Digital World », (2002) 5-3 *Information, Communication & Society* 382.

REIMAN, Jeffrey H., « Privacy, Intimacy and Personhood », (1976) 6-1 *Phil. & Pub. Aff.* 26.

RENKE, Wayne N., « Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy », (2006) 43-3 *Alta. L. Rev.* 779.

RICHARDS, Neil M., « The Dangers of Surveillance », (2013) 126-7 *Harv. L. Rev.* 1934.

SAMSON, Mélanie, « Interprétation large et libérale et interprétation contextuelle : convergence ou divergence? », (2008) 49 *C. de D.* 297.

SCASSA, Teresa, « Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy », (2010) 7 *Can. J. L. & Tech.* 193.

TIEN, Lee, « Privacy, Technology and Data Mining », (2004) 30 *Ohio N. U. L. Rev.* 389.

TREMBLAY, Luc B., « L'interprétation téléologique des droits constitutionnels », (1995) 29 *R.J.T.* 459.

WARREN, Samuel D. et Louis D. BRANDEIS, « The Right to Privacy », (1890) 4-5 *Harv. L. Rev.* 193.

Rapports et documents gouvernementaux

CANADA. BUREAU DU CONSEIL PRIVE, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Ottawa, Bureau du Conseil privé, 2004, en ligne : <http://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf>.

CLARKE, Richard A., Michael J. MORELL, Geoffrey R. STONE, Cass R. SUNSTEIN et Peter SWIRE, *Liberty and Security in a Changing World*, President's Review Group on Intelligence and Communications Technologies, 2013, en ligne : <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

COMITE CANADIEN DE LA REFORME PENALE ET CORRECTIONNELLE, *Rapport du Comité canadien de la réforme pénale et correctionnelle. Justice pénale et correction : un lien à forger*, Ottawa, Imprimeur de la Reine pour le Canada, 1969, en ligne : <http://www.johnhoward.ca/media/%281969%29%20HV%208395%20A6%20C33%201969%20F%20%28Ouimet%29.pdf>.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, « Total Information Awareness (TIA) System », en ligne :

<http://web.archive.org/web/20021003053651/http://www.darpa.mil/iao/tiasystems.htm>.

ÉTATS-UNIS, ROYAUME-UNI, CANADA, AUSTRALIE et NOUVELLE-ZELANDE, TOP SECRET, *Amendment no. 4 to the appendices to the UKUSA Agreement*, LSIB/141/55, 1955, en ligne : <https://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf>.

GROUPE D'ETUDE ETABLI CONJOINTEMENT PAR LE MINISTERE DES COMMUNICATIONS ET LE MINISTERE DE LA JUSTICE, *L'ordinateur et la vie privée*, Ottawa, Information Canada, 1972.

NATIONAL SECURITY AGENCY, *UKUSA Agreement Release 1940-1956*, en ligne : <https://www.nsa.gov/public_info/declass/ukusa.shtml>.

OTTAWA, SECRETARIAT DU CONSEIL DU TRESOR DU CANADA, *Métadonnées*, 2012, en ligne : <http://www.tbs-sct.gc.ca/im-gi/imrc-crgi/metadata-metadonnees-fra.asp>.

OTTAWA, TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *TERMIUM Plus*, « Métadonnée », 2011, en ligne : <http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=&index=alt&__index=alt&srchtxt=m%E9tadonn%E9e&comencsrch.x=0&comencsrch.y=0>.

PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, *The Challenge of Crime in a Free Society*, Washington, D.C., United States Government Printing Office, 1967, en ligne : <https://www.ncjrs.gov/pdffiles1/nij/42.pdf>.

QUEBEC, OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2002, en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8869869>.

UNITED STATES DEPARTMENT OF DEFENSE'S TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, *Safeguarding Privacy in the Fight Against Terrorism*, 2004, en ligne : <http://epic.org/privacy/profiling/tia/tapac_report.pdf>.

Rapports non gouvernementaux

CARDOZO, Nate, Cindy COHN, Parker HIGGINS, Kurt OPSAHL et Rainey REITMAN, *Who has your back? Protecting Your Data from Government Requests*, Electronic Frontier Foundation, 2014, en ligne : <https://www.eff.org/files/2014/05/19/who-has-your-back-2014-govt-data-requests.pdf>.

CAVOUKIAN, Ann, *Privacy by Design. Strong Privacy Protection – Now, and Well into the Future*, 2011, en ligne : <http://www.ipc.on.ca/images/Resources/PbDReport.pdf>.

CONLEY, Chris, *Metadata. Piecing Together a Privacy Solution*, San Francisco, American Civil Liberties Union of California, 2014, en ligne : <https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf>.

ELECTRONIC FRONTIER FOUNDATION, « Secure Messaging Scorecard » (6 novembre 2014), en ligne : <https://www.eff.org/secure-messaging-scorecard>.

HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40, 23e sess., 2013, en ligne : <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement>.

HUMAN RIGHTS WATCH et AMERICAN CIVIL LIBERTIES UNION, *With Liberty to Monitor All. How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*, Human Rights Watch, 2014, en ligne : <https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf>.

Articles de journaux

BAMFORD, James, « The Agency that could be Big Brother », *The New York Times* (25 décembre 2005), en ligne : <http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=all&_r=1&>.

BBC NEWS, « Sydney siege: Hostages held in Lindt cafe », *BBC News* (15 décembre 2014), en ligne : <http://www.bbc.com/news/world-australia-30473983>.

———, « Charlie Hebdo attack: Three days of terror », *BBC News* (14 janvier 2015), en ligne : <http://www.bbc.com/news/world-europe-30708237>.

BOWCOTT, Owen, « UK intelligence agencies spying on lawyers in sensitive security cases », *The Guardian* (7 novembre 2014), en ligne : <http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq>.

BRANDIS, George, « The more intelligence I read, the more conservative I become », *The Guardian* (18 avril 2014), en ligne : <http://www.theguardian.com/commentisfree/2014/apr/09/the-more-intelligence-i-read-the-more-conservative-i-become>.

DAVIS, Kenan, Nadja POPOVICH, Kenton POWELL et Ewen MACASKILL, « NSA Files : Decoded », *The Guardian* (1 novembre 2013), en ligne : <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

FREEZE, Colin, « Data-collection program got green light from MacKay in 2011 », *The Globe and Mail* (10 juin 2013), en ligne : <http://www.theglobeandmail.com/news/politics/data-collection-program-got-green-light-from-mackay-in-2011/article12444909/>.

———, « Raw documents : Canada's 'top secret' data mining program », *The Globe and Mail* (10 juin 2013), en ligne : <http://www.theglobeandmail.com/news/national/raw-documents-canadas-top-secret-data-mining-program/article12446852/?from=12444909>.

GALLAGHER, Ryan, « The Surveillance Engine: How The Nsa Built its Own Secret Google », *The Intercept* (25 août 2014), en ligne : <https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>.

GELLMAN, Barton, « U.S. surveillance architecture includes collection of revealing Internet, phone metadata », *The Washington Post* (15 juin 2013), en ligne : <http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_print.html>.

GELLMAN, Barton et Ashkan SOLTANI, « NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say », *The Washington Post* (30 octobre 2013), en ligne : <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>.

GREENWALD, Glenn, « The crux of the NSA story in one phrase: "collect it all" », *The Guardian* (15 juillet 2013), en ligne : <http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all>.

———, « Glenn Greenwald: The NSA's 'collect it all' mission », *National Post* (2 mai 2014), en ligne : <http://fullcomment.nationalpost.com/2014/05/02/glenn-greenwald-the-nsas-collect-it-all-mission/>.

———, « Congress Is Irrelevant on Mass Surveillance. Here's What Matters Instead », *The Intercept* (19 novembre 2014), en ligne : <https://firstlook.org/theintercept/2014/11/19/irrelevance-u-s-congress-stopping-nsas-mass-surveillance/>.

GREENWALD, Glenn et Spencer ACKERMAN, « NSA collected US email records in bulk for more than two years under Obama », *The Guardian* (juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama>.

———, « How the NSA is still harvesting your online data », *The Guardian* (27 juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection>.

GREENWALD, Glenn et Ewen MACASKILL, « NSA Prism program taps into user data of Apple, Google, and others », *The Guardian* (7 juin 2013), en ligne : <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

GREER, Evan, « How the USA Freedom Act failed on all fronts », *The Guardian* (19 novembre 2014), en ligne : <http://www.theguardian.com/media-network/2014/nov/19/how-usa-freedom-act-failed-on-all-fronts>.

GUARDIAN US INTERACTIVE TEAM, « A Guardian guide to your metadata », *The Guardian* (12 juin 2013), en ligne : <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1000001>.

LEE HOTZ, Robert, « The Really Smart Phone », *The Wall Street Journal* (23 avril 2011), en ligne : <http://online.wsj.com/news/articles/SB10001424052748704547604576263261679848814>.

NAKASHIMA, Ellen et Ed O'KEEFE, « Senate fails to advance legislation on NSA reform », *The Washington Post* (18 novembre 2014), en ligne : <http://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html>.

NAKASHIMA, Ellen et Joby WARRICK, « For NSA chief, terrorist threat drives passion to 'collect it all' », *The Washington Post* (14 juillet 2013), en ligne : <http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html>.

O'KEEFE, Ed, « Transcript: Dianne Feinstein, Saxby Chambliss explain, defend NSA phone records program », *The Washington Post* (6 juin 2013), en ligne : <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/>.

PAYTON, Laura, « Anti-terrorism powers: What's in the legislation? », *CBC News* (30 janvier 2015), en ligne : <http://www.cbc.ca/news/politics/anti-terrorism-powers-what-s-in-the-legislation-1.2937964>.

PETERSON, Andrea, « LOVEINT: When NSA officers use their spying power on love interests », *The Washington Post* (24 août 2013), en ligne :

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/>.

REVAULT D'ALLONNES, David et Bastien BONNEFOUS, « Manuel Valls annonce la création de 2 680 postes pour lutter contre le terrorisme », *Le Monde* (21 janvier 2015), en ligne : <http://www.lemonde.fr/politique/article/2015/01/21/manuel-valls-annonce-la-creation-de-2680-emplois-pour-lutter-contre-le-terrorisme_4560334_823448.html>.

SANCHEZ, Julian, « Obama Backs Off Real NSA Reforms », *The Daily Beast* (15 janvier 2014), en ligne : <http://www.thedailybeast.com/articles/2014/01/15/obama-backs-off-real-nsa-reform.html>.

WATT, Nicholas, Rowena MASON et Ian TRAYNOR, « David Cameron pledges anti-terror law for internet after Paris attacks », *The Guardian* (12 janvier 2015), en ligne : <http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg>.

WINGROVE, Josh, Steven CHASE, Bill CURRY et Jill MAHONEY, « Attack on Ottawa : PM Harper cites terrorist motive », *The Globe and Mail* (22 octobre 2014), en ligne : <http://www.theglobeandmail.com/news/politics/parliament-shooting/article21217602/>.

ZELLER, Tom, « Ideas & Trends; Cloak, Dagger, Echelon », *The New York Times* (16 juillet 2000), en ligne : <http://www.nytimes.com/2000/07/16/technology/ideas-trends-cloak-dagger-echelon.html>.

Sites Internet

Blackphone, en ligne : <https://www.blackphone.ch/#introduction>.

Silent Circle, en ligne : <https://silentcircle.com/services>.

Open WhisperSystems, en ligne : <https://whispersystems.org/>.

RetroShare, en ligne : <http://retroshare.sourceforge.net/index.html>.

Allocutions

MCLACHLIN, Beverley, *Lutter contre le terrorisme tout en préservant nos libertés civiles*, allocution prononcée devant le Ottawa Women's Canadian Club, 22 septembre 2009, en ligne : http://www.scc-csc.gc.ca/court-cour/judges-juges/spe-dis/bm-2009-09-22-fra.aspx.

OBAMA, Barack, « Statement by the President », *The White House, Office of the Press Secretary* (7 juin 2013), en ligne : <http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president>.

TRUDEAU, Pierre Elliott, *Allocution lors de la Cérémonie de proclamation*, 17 avril 1982, en ligne : <http://www.collectionscanada.gc.ca/premiersministres/h4-4024-f.html>.

Autres documents

AMNISTIE INTERNATIONALE, « New tool for spy victims to detect government surveillance » (20 novembre 2014), en ligne : <http://www.amnesty.org/en/news/new-tool-spy-victims-detect-government-surveillance-2014-11-20>.

ELECTRONIC FRONTIER FOUNDATION, « Surveillance Self-Defense », en ligne : <https://ssd.eff.org/en>.

ELECTRONIC FRONTIER FOUNDATION, « International Principles on the Application of Human Rights to Communications Surveillance » (mai 2014), en ligne : <https://en.necessaryandproportionate.org/>.

FORCESE, Craig, « Metastasized Metadata: More On The CSEC Ministerial Authorization », *National Security Law Blog* (12 juin 2013), en ligne : <http://craigforcese.squarespace.com/national-security-law-blog/2013/6/12/metastasized-metadata-more-on-the-csec-ministerial-authoriza.html>.

HORTON, Scott, « Madison on the Dangers of War », *Harper's Magazine* (7 juillet 2007), en ligne : <http://harpers.org/blog/2007/07/madison-on-the-dangers-of-war/>.

KURL, Shachi, *More Canadians, Britons & Americans view Edward Snowden as « hero » than « traitor »,* Angus Reid Global, 2013, en ligne : <http://www.angusreidglobal.com/wp-content/uploads/2013/10/2013.10.30-Snowden-Leaks.pdf>.

SOLZHENITSYN, Aleksandr, *Cancer Ward*, Londres, Vintage, 2003.