Chronique – L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements

Jean-François DE RICO*

EYB2014REP1480 (approx. 19 page(s))

EYB2014REP1480

Repères, Février 2014

Jean-François DE RICO*
Chronique – L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements

Indexation

ACCÈS À L'INFORMATION ; ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ; PROTECTION DES RENSEIGNEMENTS PERSONNELS ; COMMUNICATIONS ; TECHNOLOGIES DE L'INFORMATION ; *LOI CONCERNANT LE CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION* ; PÉNAL ; TERRORISME ; ATTEINTES À LA VIE PRIVÉE ; INTERCEPTION DE COMMUNICATIONS PRIVÉES ; FOUILLES, PERQUISITIONS OU SAISIES ; PERQUISITION AVEC MANDAT ; EXÉCUTION DU MANDAT ; FAÇON D'EXÉCUTER LE MANDAT ; USAGE D'UN SYSTÈME INFORMATIQUE ; PROCÉDURE ET POUVOIRS SPÉCIAUX ; ORDONNANCE DE COMMUNICATION ; ORDONNANCE D'ASSISTANCE ; DROIT COMPARÉ

TABLE DES MATIÈRES

Résumé

Le recours à des services en mode infonuagique soulève plusieurs enjeux juridiques liés à la gestion de l'information, dont ceux relatifs à la protection des renseignements personnels. L'auteur analyse ici l'étendue des obligations imposées par les lois québécoises aux organisations qui considèrent l'opportunité de recourir aux services de prestataires issus ou utilisant des installations dans d'autres juridictions, notamment en regard des risques associés aux droits d'accès accordés aux autorités gouvernementales.

INTRODUCTION

Le *cloud computing*, que l'Office québécois de la langue française nous invite à traduire par le terme « infonuagique », ne désigne pas spécifiquement une technologie, mais plutôt une nouvelle façon d'accéder et d'utiliser des ressources ou services informatiques. L'épithète « nouvelle » est par ailleurs discutable puisque ce mode d'accès est disponible et largement utilisé en regard de certains types de services tels que les applications de courriels depuis le milieu des années 1990.

L'infonuagique consiste essentiellement à accéder et à utiliser des ressources informatiques distantes par l'entremise d'un réseau étendu. Le Commissariat à la protection de la vie privée du Canada a adopté la définition suivante, élaborée par le *National Institute of Standards and Technology* des États-Unis :

> L'infonuagique est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services. [1]

Rendue possible par la hausse de capacité, la rapidité et la robustesse des réseaux, et propulsée par l'attrait du modèle d'affaires qui permet aux organisations d'éviter les immobilisations et de réduire les efforts liés à la gestion, à l'entretien et au support des ressources informatiques, l'industrie de l'infonuagique connaît une croissance marquée depuis plusieurs années. Une firme de recherche prévoit que la proportion des données de consommateurs stockées en ligne passera de 7 % en 2011 à 36 % en 2016 [2].

Bien que la nature, l'étendue et la portée des services et ressources rendus disponibles aient beaucoup évolué, la logique de délocalisation et d'accès à des ressources centralisées n'est pas nouvelle. En effet, la possibilité d'interconnecter les ordinateurs du département de la défense américaine dans les années 1960 et la volonté d'élargir l'accès aux capacités de calculs de quelques superordinateurs aux fins des universités et centres de recherches américains dans les années 1980 ont respectivement été deux des principaux moteurs de développement du réseau Internet [3].

Néanmoins, la possibilité de recourir à des équipements et ressources externes pour tout l'éventail des services informatiques, que ce soit l'hébergement web, le serveur de téléphonie, le stockage ou l'utilisation de logiciels de bureautique, est un phénomène récent [4].

Du point de vue juridique, le recours à des services de technologies de l'information en infonuagique impliquant la communication ou le transfert aux fins de traitement ou d'hébergement de document revêtant un caractère confidentiel dont des renseignements personnels, commande une analyse de plusieurs enjeux juridiques relatifs à la gestion et à la sécurité de l'information, ainsi qu'à la protection des renseignements personnels. On pense notamment à l'examen des conditions permettant aux organisations de faire face à leurs obligations imposées par la *Loi concernant le cadre juridique des technologies de l'information* quant au maintien de l'intégrité, à la disponibilité et à la sécurité des documents hébergés en mode infonuagique, ainsi qu'aux conditions imposées par les lois sur la protection des renseignements personnels pour le transfert ou la communication de tels renseignements.

Depuis 2001, le *Patriot Act* a été maintes fois identifié comme un risque d'accès et de communication non autorisés qui militait contre le recours à des prestataires de services américains ou ayant des liens avec des prestataires de services américains. Les positions avancées sur ce sujet s'inscrivent souvent dans un examen de la possibilité de recourir à des prestataires américains de services en mode infonuagique en vertu des obligations imposées par les lois sur la protection des renseignements personnels, dont le libellé, du moins dans le cas de la loi régissant le secteur public au Québec, peut paraître équivoque.

Aux fins de cet article, nous réviserons l'encadrement juridique du recours à des services infonuagiques pour les organisations publiques et privées québécoises en nous attardant aux obligations qui leur incombent relativement à la protection des renseignements personnels lorsqu'elles confient de tels renseignements à des tiers, ainsi qu'aux

enjeux soulevés par les droits d'accès accordés aux autorités américaines en les comparant à ceux accordés par les lois canadiennes. Nous ne procéderons pas ici à l'analyse des conditions d'utilisation de prestataires de services infonuagiques[5].

Les documents rendus publics par Edward Snowden au cours de l'année 2013 ont révélé l'étendue des autorisations accordées par le Foreign Intelligence Surveillance Tribunal et des opérations de surveillance effectuées en vertu des pouvoirs accordés aux autorités américaines, et permettent de jeter un regard plus éclairé sur les dispositions législatives en cause.

Notre analyse aborde principalement les textes de loi et les rares interprétations qu'ont pu en faire les tribunaux. Nous ne procéderons pas ici à un examen détaillé des programmes de surveillance des agences de renseignements américaines qui ont été révélées par Edward Snowden au cours de l'année 2013[6]. Sans vouloir ignorer cette réalité, il nous apparaît que l'état de la situation n'est pas encore complètement connu[7]. Au surplus, deux tribunaux fédéraux américains de première instance ont rendu, en décembre 2013, des jugements qui semblent *a priori* contradictoires[8] en regard de la constitutionnalité des opérations d'interception de communications, et, finalement, l'implication des gouvernements des alliés des États-Unis, dont le Canada, dans les différentes opérations demeure nébuleuse.

Nous nous contenterons de référer aux grandes lignes des révélations faites en 2013 afin d'illustrer l'exercice qui a été fait des pouvoirs accordés par les lois américaines, et de tenter de déterminer, à la lumière des droits d'accès accordés aux autorités canadiennes, si :

> i) ces droits d'accès sont tels qu'une organisation québécoise devrait nécessairement conclure que les renseignements confiés à un prestataire de services infonuagiques américain ou ayant des installations ou activités aux États-Unis ne bénéficieraient pas d'une protection équivalant à celle prévue par la loi québécoise applicable ; ou si,
>
> ii) l'exercice de ces droits d'accès est assimilable à une communication à « un organisme qui est chargé de prévenir, détecter ou réprimer le crime ou les infractions » au sens des lois sur la protection des renseignements personnels québécoises.

I– CADRE JURIDIQUE

Le droit à la vie privée, dont la protection des renseignements personnels est l'une des composantes, est reconnu à titre de droit fondamental par les chartes canadiennes et québécoises[9]. Le principe de la confidentialité des renseignements personnels et les responsabilités des parties qui les recueillent sont quant à eux énoncés dans plusieurs lois d'application générale ainsi que dans des lois et règlements spécifiques à différentes sphères d'activités, tels que les services financiers ou les services de santé.

Aux fins des questions qui nous préoccupent ici, le cadre juridique d'application générale est défini par la *Loi concernant le cadre juridique des technologies de l'Information* (LCCJTI)[10], ainsi que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LADOPPRP)[11] ou *la Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP)[12] ainsi que les dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) relatives aux transferts transfrontaliers pour les organisations du secteur privé[13]. Il est important de noter que plusieurs lois applicables à des domaines d'activités spécifiques peuvent moduler les règles prévues par les lois d'application générale.

A. La Loi sur le cadre juridique des technologies de l'information

La *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI) comporte une section intitulée « Maintien de l'intégrité du document au cours de son cycle de vie » dans laquelle le législateur impose des obligations à la partie qui s'en remet aux services d'un tiers pour l'hébergement, la conservation ou la transmission de documents[14].

L'article 25 de la LCCJTI énonce l'obligation de la personne responsable de l'accès de mettre en place des mesures de sécurité pour assurer la confidentialité des documents qui revêtent un tel caractère. L'article 26 prévoit, par ailleurs, que la personne qui confie un document à un tiers « *pour qu'il en assure la garde* » doit préalablement informer celui-ci du caractère confidentiel du document, de la protection qu'il requiert et des personnes habilitées à en prendre connaissance. Le même article impose au prestataire l'obligation de mettre en place « les moyens technologiques convenus [...] pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance » et de respecter toute autre obligation légale relative à la conservation documentaire.

Cet article a pour effet d'imposer aux organisations québécoises l'obligation de stipuler expressément la nature des documents à caractère confidentiel qu'elle confie ou qu'elle est susceptible de confier à un prestataire de services et de prévoir des mesures ou des processus afin d'en assurer la sécurité. Bien que cette disposition n'ait jamais été interprétée, son libellé nous semble requérir plus que la formule contractuelle de base standard référant aux « meilleures pratiques de l'industrie ».

La LCCJTI traite également des obligations applicables à la transmission d'un document technologique qui revêt un caractère confidentiel[15]. L'article 34 de la LCCJTI prévoit que la confidentialité doit être préservée par un moyen approprié au mode de transmission, et impose de conserver la documentation « expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis [...] ». À cet égard, un contrat de services infonuagiques qui comporte une facette de transmission devrait prévoir le mécanisme (par ex. : le chiffrement) utilisé pour maintenir la confidentialité des documents transmis.

B. Les lois sur la protection des renseignements personnels

À l'instar de la loi fédérale[16], les lois québécoises applicables aux secteurs publics et privés réfèrent toutes deux à la possibilité pour une organisation de recourir aux services d'un tiers pour le traitement de documents comportant des renseignements personnels :

LPRPSP	LADOPPRP
20. Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant ou à toute partie à un contrat de service ou d'entreprise qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ou de son contrat.	67.2. Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme. [...]

L'article 67.2 de la loi applicable au secteur public précise de plus l'obligation de l'organisation de conclure un contrat écrit, d'y mentionner les dispositions applicables de la loi, d'y prévoir les mesures destinées à assurer le maintien de la confidentialité des renseignements personnels et d'obtenir des engagements de confidentialité. Quant à la loi appliquée au secteur privé, la Commission d'accès à l'information a interprété l'article 20 LPRPSP comme exigeant la conclusion d'un contrat écrit[17].

Les deux lois québécoises prévoient par ailleurs la possibilité de recourir aux services d'un prestataire dont les installations sont sises à l'extérieur du Québec aux fins de détention, d'utilisation ou de communication pour son compte :

LPRPSP (secteur privé)	LADOPPRP (secteur public)
17. La personne qui exploite une entreprise au Québec et qui communique à l'extérieur du Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer : [...] 1° que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées sauf dans des cas similaires à ceux prévus par les articles 18 et 23 ; 2° dans le cas de listes nominatives [...]. Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1° et 2°, elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.	70.1. Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi. Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

Aux fins de notre analyse, nous partons de la prémisse selon laquelle la locution « communiquer ou confier, à une personne à l'extérieur du Québec des renseignements personnels, la tâche de les détenir, les utiliser ou les communiquer » est suffisamment large pour englober des services d'hébergement de documents[18].

Alors que la loi applicable au secteur privé impose l'obligation de « prendre tous les moyens raisonnables pour s'assurer [...] que les renseignements bénéficieront des conditions prévues aux paragraphes 1 et 2 [de l'article] », la loi applicable au secteur public utilise le libellé « doit s'assurer [que les renseignements] bénéficieront d'une protection équivalente à celle prévue à la présente loi », ce qui est indicatif d'une obligation plus large pour l'organisation publique. Il est important de noter que ces obligations s'appliquent indépendamment du degré de sensibilité des renseignements visés.

Ces articles soulèvent une difficulté d'interprétation relative à l'étendue des obligations qui incombent aux organisations considérant l'opportunité de recourir à des services en mode infonuagique en vertu de ces articles. Deux thèses principales qui ne s'excluent pas nécessairement l'une et l'autre peuvent être formulées[19]. Selon le cas, ces articles imposeraient :

- L'obligation de procéder à un examen détaillé de l'encadrement juridique du territoire visé afin de déterminer si les lois applicables prévoient une protection équivalente ;
- La conclusion d'une entente contractuelle comportant des dispositions contractuelles permettant de se conformer aux obligations énoncées respectivement par les articles 17 et 70.1.

Nous pouvons d'emblée écarter la possibilité de se contenter de la conclusion d'une entente de services puisque la voie contractuelle ne pourrait contrer l'application ou avoir préséance sur une loi d'ordre public qui serait irréconciliable avec les conditions prévues à l'article 17 de la LPRPSP ou avec la LADOPPRP. Des conditions d'utilisation stipulant le maintien de la confidentialité en toutes circonstances ne pourraient faire échec à l'application d'une loi accordant des droits d'accès tous azimuts, ou à l'exercice de prérogatives exécutives non encadrées par la loi.

Selon nos vérifications, la Commission d'accès à l'information du Québec n'a émis aucune ligne directrice ou document faisant état de son interprétation de l'étendue de l'obligation qui incombe aux organisations en vertu des articles 17 de la LPRPSP ou 70.1 de la LADOPPRP. Par ailleurs, bien que nos recherches ne soient pas exhaustives de ce côté, nous n'avons répertorié aucune directive émanant du secrétariat du Conseil du trésor relativement à l'application de l'article 70.1 de la LADOPPRP.

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) reconnaît également la possibilité de confier des renseignements personnels à un tiers. Le principe 4.1.3 de l'annexe I énonce : « Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ». Cette Loi fédérale et la loi québécoise applicable au secteur privé ont été jugées essentiellement similaires par le gouvernement canadien[20].

Là où la loi québécoise applicable au secteur privé réfère « au bénéfice des conditions prévues [à l'article 17] », la LPRPDE réfère à la notion de « degré comparable de protection ». L'exigence de la LPRPDE nous apparaît ainsi énoncer une exigence similaire de façon moins spécifique[21]. Le commissariat à la protection de la vie privée du Canada semble considérer que seule la LPRPDE devrait s'appliquer en cas de transfert transfrontalier. Avec égard, cette position nous semble porteuse de plus d'inconvénients que d'avantages, et il nous apparaît *a priori* que les dispositions en cause ne sont nullement incompatibles, et que, dans la mesure où les deux lois sont valides, la théorie de la prépondérance fédérale ne saurait trouver application[22].

Dans un document intitulé *Lignes directrices sur le traitement transfrontalier des données personnelles*, le Commissariat à la protection de la vie privée du Canada explique la notion de « Degré comparable de protection » de la façon suivante : « La tierce partie qui traite les renseignements doit fournir une protection comparable au niveau de protection qui serait fourni si l'information n'avait pas été transférée. Cela ne veut pas dire que les mesures de protection devraient être les mêmes partout, mais qu'elles devraient généralement s'équivaloir »[23].

Dans le résumé des conclusions de l'enquête no 2005-313 relative au recours aux services d'un fournisseur américain par un émetteur de cartes de crédit canadien, le Commissariat à la protection de la vie privée du Canada a référé aux lignes directrices du Bureau du surintendant des institutions financières (BSIF)[24], en vertu desquelles une banque peut être soustraite à l'obligation de conservation documentaire au Canada imposée par les articles 239 et 597 de la *Loi sur les banques*[25]. Aux termes de ces lignes directrices, en cas d'impartition de services à l'extérieur du Canada, l'organisation visée doit « accorder une attention particulière aux exigences juridiques du territoire en question »[26]. Sous la rubrique « 7.2 Politiques et procédures de gestion des risques liés aux ententes d'impartition importantes », le document énonce : « [...] le programme de gestion des risques [doit] tenir compte de toute préoccupation additionnelle ayant trait au contexte économique et politique, à l'avancement technologique et au

profil de risque juridique et réglementaire du territoire étranger ».

Après avoir référé au libellé de cette ligne directrice, lequel est plus précis que les lois québécoises et indicatif d'une obligation de vérification de l'environnement juridique certainement plus exigeante que celles qui seraient, le cas échéant, énoncées dans les lois québécoises et dans la LPRPDE, le Commissariat à la protection de la vie privée du Canada écrit :

> Dans les cas d'impartition à un pays étranger, la LPRPDE *n'exige pas* une comparaison exhaustive entre les lois canadiennes et les lois étrangères. Elle *exige* par contre que les organisations prennent en considération tous les éléments entourant la transaction. L'organisation pourrait ainsi se rendre compte qu'il serait mal avisé de procéder à certains transferts en raison de la nature instable d'un régime étranger. Dans d'autres cas, les renseignements se révèlent de nature si délicate qu'ils ne devraient être envoyés à aucune administration étrangère. [27]

Le secrétariat du Conseil du trésor du Canada a également publié un document d'orientation destiné aux organismes fédéraux sur les ententes d'échange de renseignements personnels qui comporte un chapitre portant sur les considérations transfrontières. Ce document d'orientation aborde notamment le risque découlant des lois antiterroristes tout en proposant une approche d'analyse et de gestion de ce risque [28].

Bien que les conclusions d'enquête et les lignes directrices du Commissariat ne soient pas déterminantes en regard de l'interprétation qu'un tribunal pourrait faire des dispositions des lois québécoises, elles tendent à appuyer la thèse selon laquelle une analyse exhaustive n'est pas requise aux termes des articles 17 et 70.1 des lois québécoises.

Il y a lieu de noter que le dernier alinéa de l'article 17 de la LPRPSP et l'article 70.1 de la loi applicable au secteur public découlent de modifications apportées à ces lois en 2006 [29]. Alors qu'au moment du dépôt et de l'adoption de la loi modificatrice, les débats découlant du *Patriot Act* étaient engagés, que l'approche du Commissariat fédéral était connue, que les parlementaires réfèrent directement à la loi honnie, ni l'article 17 ni l'article 70.1 n'imposent d'obligation spécifique d'analyse juridique. Au surplus, l'examen des débats parlementaires portant sur l'article du projet de loi 86 ayant mené à l'introduction de l'article 70.1 et du dernier alinéa de l'article 17 permet de discerner chez certains membres de la commission parlementaire faisant partie de l'opposition à ce moment, la volonté d'éviter l'accès aux renseignements personnels conservés par les organisations québécoises par les autorités américaines et de faire échec au *Patriot Act* [30], le libellé des articles 17 et 70.1 qui a été retenu ne permet pas, selon nous, d'attribuer au législateur l'intention d'interdire le recours à des fournisseurs américains ou à des fournisseurs utilisant des installations ou ayant un établissement aux États-Unis [31].

Ainsi, la LPRPSP et la LADOPPRP n'interdisent pas de recourir à des prestataires de services d'autres juridictions, et ne subordonnent pas le recours à un prestataire de services en mode infonuagique utilisant des installations à l'extérieur du Québec à l'obtention d'un consentement spécifique des personnes concernées.

Les articles 17 et 20 de la LPRPSP et 67.2 et 70.1 LADOPPRP imposent au surplus au détenteur des renseignements personnels l'obligation de conclure un contrat écrit et de s'assurer que les renseignements personnels reçoivent une protection équivalente à celle prévue par les dispositions expressément visées de la LPRPSP et la les dispositions de la LADOPPRP dans le cas des organismes publics.

Nous considérons quant à nous que cette obligation peut être satisfaite par une révision de l'encadrement juridique de la protection des renseignements personnels dans la juridiction visée afin de déterminer s'il existe un tel encadrement, si celui-ci reconnaît le droit à la vie privée et le principe de la confidentialité des renseignements personnels, et si celui-ci comporte des règles irréconciliables avec la loi québécoise applicable. Dans le cas où les lois applicables ne comportent pas d'éléments irréconciliables, le contrat de services devrait stipuler les engagements nécessaires pour combler, le cas échéant, les lacunes de la loi locale, et préciser les obligations du fournisseur de services en ce qui a trait à la protection des renseignements personnels et au maintien de la confidentialité des documents qui lui sont confiés.

Cette interprétation rejoint, par ailleurs, les positions prises par le Commissariat à la protection de la vie privée du Canada dès 2006 et réitérées en janvier 2014 [32] ainsi qu'à celle privilégiée par d'autres auteurs [33].

Le libellé de l'article 8(3) de la loi applicable au secteur privé [34] et le principe de transparence de façon générale (Principe 8 – Annexe I – LPRPDE) prescrivent, toutefois, l'obligation de l'organisation d'aviser les personnes concernées, du fait ou de la possibilité que leurs renseignements personnels soient conservés, ou transférés à des fins de conservation, à l'extérieur du Québec, et qu'ils soient dès lors sujets aux droits d'accès des gouvernements en vertu des pouvoirs qui leur sont accordés par les lois applicables. Les organismes publics doivent par ailleurs tenir et diffuser sur leur site Internet un registre des « communications » faites à des prestataires de services [35].

Nous présentons ci-dessous un sommaire du régime juridique relatif au respect de la vie privée et à la protection des renseignements personnels aux États-Unis ainsi qu'une analyse sommaire des droits d'accès accordés par les lois américaines. Afin d'apprécier le bien-fondé des craintes fréquemment soulevées à l'égard du *Patriot Act*, nous avons procédé à un examen comparatif de ceux-ci avec les droits d'accès accordés aux autorités gouvernementales canadiennes.

Notre première conclusion sur la portée des articles 17 LPRPSP et 70.1 LADOPPRP soulève une question importante en regard de ce qui devrait être considéré comme un environnement juridique irréconciliable. Les obligations imposées par ces articles relativement à l'équivalence de la protection offerte dans une autre juridiction réfèrent dans le cas de la loi applicable au secteur privé à la protection accordée par la règle de non-communication sous réserve des exceptions à celle-ci prévues aux articles 18 et 23 et à la protection accordée par la LADOPPRP dans le cas du secteur public, et non pas à l'ensemble des lois applicables au Québec. Ces articles ne subordonnent donc pas la possibilité de conclure à l'existence d'une protection équivalente à la similarité de toutes les dispositions légales susceptibles de constituer une exception aux règles de protection de la confidentialité des renseignements personnels.

À cet égard, il est important de noter qu'à l'instar de la majorité des législations vouées à la protection des renseignements personnels, les deux lois québécoises énoncent des exceptions à l'interdiction de communication, en regard de toute communication « à un organisme chargé en vertu de la loi de prévenir, détecter ou réprimer le crime ou les infractions aux lois, qui le requiert dans l'exercice de ses fonctions, si le renseignement est nécessaire pour la poursuite d'une infraction à une loi applicable au Québec » (art. 18(3) LPRPSP et 59(3) LADOPPRP).

L'appréciation de la protection dont peuvent bénéficier les renseignements personnels confiés à un fournisseur soumis à une juridiction étrangère, notamment quant aux droits d'accès des gouvernements, doit donc être faite en tenant compte de cette exception.

II– DROITS D'ACCÈS DES AUTORITÉS GOUVERNEMENTALES AMÉRICAINES ET CANADIENNES

A. Encadrement juridique de la protection des renseignements personnels aux États-Unis

Aux États-Unis, le fondement juridique de la protection des renseignements personnels se trouve dans le quatrième amendement de la constitution [36]. Ce texte constitutionnel a été interprété de façon à assurer le droit à la sécurité et à la dignité de la personne, et à protéger l'individu contre l'intrusion de l'État [37].

Cette protection bénéficie aux citoyens américains et aux étrangers ayant développé « such ties with the United States that they form part of the national community » et non pas à des citoyens d'un autre pays qui seraient clients d'un fournisseur de services américain ou ayant un établissement aux États-Unis. Il subsiste au surplus une incertitude à savoir si la protection constitutionnelle s'étend à des données électroniques à compter du moment où elles sont confiées à un tiers, tel qu'un fournisseur de services Internet. La jurisprudence de la Cour suprême des États-Unis a déjà établi que cette protection constitutionnelle ne s'étend pas à une information une fois qu'elle est communiquée à un tiers [38].

Le droit à la vie privée et à la protection de ce que nous désignons comme des « renseignements personnels » dans le cadre des relations entre parties privées, a été

invoqué par la doctrine américaine dès 1890 et ensuite établi par la jurisprudence qui a notamment reconnu des causes d'action en responsabilité civile pour atteinte à la vie privée [39].

En 1973, le gouvernement américain a élaboré des lignes directrices sous la forme de huit principes désignés comme les *Fair Information Practice Principles* (FIPPs) [40]. Les huit principes recoupent ceux identifiés par l'OCDE dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* [41], ainsi que les principes énoncés dans la *Norme nationale du Canada intitulée Code type sur la protection des renseignements personnels* (can/csa-q830-96), énoncés dans l'annexe I de la LPRPDE.

La plupart des politiques et initiatives législatives américaines en matière de protection de la vie privée et des renseignements personnels, dont le *Privacy Act* adopté en 1974, s'appuient sur les FIPPs [42]. Cette Loi dont l'application est limitée au secteur public encadre la collecte, l'utilisation et la conservation des renseignements personnels de façon à assurer que ceux-ci ne soient recueillis que conformément et aux seules fins prévues par la loi et conservés de façon à en préserver la confidentialité [43].

À ce jour, les États-Unis n'ont pas adopté de loi d'application générale en regard du secteur privé, mais plutôt une série de lois fédérales applicables à des domaines et secteurs d'activités particuliers (communications électroniques, santé, finance, éducation, protection des enfants), et fait la promotion de codes de conduite dont l'application et le respect relèvent principalement de la *Federal Trade Commission* [44]. Différents États américains ont également adopté des lois relatives à la protection des renseignements personnels fondées sur les principes FIPPs [45].

En matière de communications électroniques, c'est une loi adoptée en 1986 qui encadre la confidentialité et la protection des renseignements personnels des utilisateurs de services de télécommunications. L'*Electronic Communication Privacy Act* applicable aux fournisseurs de services de télécommunications [46] énonce des interdictions de divulgation à titre de règles générales (art. 2702) et des droits d'accès encadrés en fonction de la nature des informations recherchées et des communications visées (art. 2703). Ces dispositions ont été interprétées de la façon suivante par une cour d'appel fédérale américaine :

> The government may obtain the contents of e-mails that are “in electronic storage” with an electronic communication service for 180 days or less “only pursuant to a warrant.” 18 U.S.C. § 2703(a). The government has three options for obtaining communications stored with a remote computing service and communications that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d). Id. § 2703(a), (b). [47]
>
> Under § 2703(b)(1)(B), the government must provide notice to an account holder if it seeks to compel the disclosure of his emails through either a § 2703(b) subpoena or a § 2703(d) order. However, § 2705 permits the government to delay notification in certain situations. [48]

Ainsi, bien que le droit constitutionnel à la vie privée ne puisse, de façon générale, bénéficier aux personnes dont les renseignements sont recueillis par les organisations québécoises, et que la protection des renseignements personnels ne soit pas assurée par une loi d'application générale et que certaines définitions du *Electronic Communication Privacy Act* [49] mériteraient d'être clarifiées [50], le corpus législatif américain reconnaît aux utilisateurs des services de télécommunications une expectative de vie privée et impose des obligations de non-divulgation aux fournisseurs de ces services.

Cet encadrement juridique n'est évidemment pas identique. Les positions prises par la Commissaire à la protection de la vie privée du Canada démontrent, néanmoins, qu'il a été considéré comme présentant une « protection comparable » ou du moins que « les mesures de protection s'équivalaient généralement » [51].

Contrairement au commissariat canadien, au mois de juillet 2000, la communauté européenne retenait l'opinion du Groupe de travail de l'article 29 [52], et concluait [53] que les lois américaines ne présentaient pas un niveau de protection adéquat au sens de la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [54]. L'objet principal de cette décision était cependant de reconnaître et de donner effet à l'approche fondée sur l'adhésion aux « principes de la “sphère de sécurité” relatifs à la protection de la vie privée ».

Or, dès juillet 2000, la commission européenne, dans la décision ayant pour effet de reconnaître que l'adhésion aux « principes de la “sphère de sécurité” relatifs à la protection de la vie privée » offrait un niveau de protection adéquat pour le transfert de données des États membres de la Communauté européenne vers les États-Unis d'Amérique, énonçait les limites d'application desdits principes :

> *L'adhésion aux principes peut être limitée par : a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis ; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir [...]* [55]

Par ailleurs, la sphère de sécurité a principalement pour objet de réitérer et rendre applicable les principes reconnus en matière de protection des renseignements personnels afin d'offrir un degré de protection similaire à celui offert par la directive européenne, et non pas à modifier ou moduler la portée des droits d'accès des gouvernements en fonction de la provenance des documents.

Tout en invoquant sa prérogative de révoquer la décision ratifiant la suffisance de la sphère de sécurité, la commission européenne a récemment présenté treize (13) recommandations visant à renforcer les principes de la sphère de sécurité dans la foulée des révélations relatives aux opérations de surveillance américaines [56], à l'égard desquelles la commission requiert l'identification de solutions de la part des États-Unis. Deux recommandations portent spécifiquement sur les droits d'Accès des autorités :

> 12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.
>
> 13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

Les droits et obligations applicables en vertu des lois américaines et des principes de la sphère de sécurité sont ainsi tempérés par les exceptions prévues par les droits d'accès accordés aux autorités gouvernementales, dont la révision est nécessaire pour considérer adéquatement l'environnement juridique de la protection des renseignements personnels aux États-Unis. Nous procédons ci-dessous à une révision sommaire des lois américaines accordant de tels droits et les comparons ensuite aux lois canadiennes.

B. Les droits d'accès accordés aux autorités gouvernementales américaines

Au cours des dernières années, les pouvoirs accordés aux termes des amendements découlant d'une loi modificatrice adoptée en 2001 sous le nom *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* [57], et à laquelle on réfère habituellement comme étant le *Patriot Act,* ont été décrits comme permettant désormais au gouvernement américain d'accéder à des données hébergées aux États-Unis ou ailleurs par l'entremise d'une filiale d'une entreprise ayant des activités et une présence américaine. Ces pouvoirs ont été invoqués, en Europe et au Canada, comme motifs justifiant d'écarter des fournisseurs américains ou de restreindre la localisation géographique des équipements destinés à héberger les systèmes, applications et données, en raison des risques de contraventions potentielles aux lois relatives à la protection des renseignements personnels qui en découleraient.

Cette Loi a d'ailleurs mené la législature de la Colombie-Britannique à modifier le *Freedom of Information and Protection of Privacy Act* [58] (FIPPA), afin d'imposer aux organisations gouvernementales l'obligation de s'assurer que les renseignements personnels qui leur sont confiés soient conservés et que l'accès à ceux-ci se fasse

uniquement du Canada.

Le *Patriot Act* était essentiellement une loi modificatrice ayant entraîné des amendements à des lois préexistantes qui conféraient des pouvoirs de surveillance et d'accès aux autorités gouvernementales américaines, dont le *Foreign Intelligence Surveillance Act* (FISA), adopté en 1978[59]. Différentes lois encadrent donc la mesure dans laquelle et la façon dont les autorités américaines peuvent accéder à des documents hébergés sur des installations sises aux États-Unis ou accessibles par des entreprises américaines :

- *Electronic Communications Privacy Act*;
- *Foreign Intelligence Surveillance Act*;
- *Computer Fraud and Abuse Act*;
- *Communications Assistance to Law Enforcement Act*;
- *Economic Espionage Act.*

Les pouvoirs qui sont habituellement dénoncés sont ceux accordés aux termes du *Foreign Intelligence Surveillance Act* (50 USC 1861 et suiv.) tel qu'amendé par le *Patriot Act* (art. 215)[60]. Les dispositions de cette Loi accordent à un tribunal spécifiquement créé pour son application (le « Tribunal FISA ») le pouvoir d'émettre *ex parte* et à huis clos des ordonnances secrètes d'interception de communication et de perquisition de toute chose ou document dans le cadre d'enquêtes relatives à la sécurité nationale, à la demande du *Federal Bureau of Investigation* (FBI).

En 2008, le *FISA Amendments Act* a de nouveau amendé le *Foreign Intelligence Surveillance Act* (50 USC 1881a et 1881b) afin de permettre au procureur général et au Director of National Intelligence de requérir une ordonnance autorisant la surveillance en regard de personnes à l'extérieur des États-Unis, ou en cas d'urgence de déposer un certificat identifiant les motifs et les cibles de la surveillance (à l'exclusion de citoyens américains).

Les rapports déposés par le procureur général pour les années 2011 et 2012 révèlent que 1745 demandes ont été présentées au Tribunal FISA pour autorisation de surveillance, interception et perquisition en 2011 et 1 856 en 2012[61].

Tel que nous le verrons ci-dessous, des pouvoirs similaires sont accordés aux juges de la Cour fédérale du Canada sur demande du Service canadien du renseignement de sécurité.

Le *Patriot Act* (art. 505) a également élargi le pouvoir accordé au FBI (*Stored Communications Act* 18 U.S. CODE § 2709) de requérir par voie de *subpoena* administratif (appelé *National Security Letters*) des informations relatives à des utilisateurs ou à des abonnés [incluant des résidents américains (*US person*)] ou à des communications en certifiant par écrit que l'information est pertinente à une enquête relative à la prévention du terrorisme. Ce droit d'accès est limité à des informations relatives à un utilisateur ou accessoires à une communication (*non content data*) et ne s'étend pas au contenu d'une communication[62]. La Loi accorde aussi au FBI le pouvoir de contraindre la partie visée de s'abstenir d'informer toute personne. Cette portion de la disposition a été jugée inconstitutionnelle par une cour fédérale au mois de mars 2013[63]. Les rapports du procureur général précités révèlent que 16 511 *subpoena* administratifs de ce type ont été émis en regard de 7 201 personnes en 2011, tandis que 15 229 l'ont été en regard de 6 223 personnes en 2012[64]. Ce droit accordé au FBI n'a pas d'équivalent en droit canadien.

Les procédures encadrant l'accès en vertu des pouvoirs plus traditionnels d'enquête de nature criminelle ont également été modifiées et varient quant à elles en fonction de certains critères. Selon le type de documents ou de données, selon l'état de la communication (transmission ou conservation), la durée de conservation, et le statut de la personne faisant l'objet de l'enquête, les autorités doivent recourir à des dispositions différentes.

Ces dispositions prévoient pour la plupart l'obligation d'émettre un *subpoena*, ou d'obtenir une ordonnance d'un tribunal ou un mandat de perquisition ou d'interception de communication. Aux termes de l'article 2703 a) b) du *Electronic Communication Privacy Act*[65], un fournisseur de services ne devrait divulguer le contenu de communications qu'en vertu d'une ordonnance ou d'un mandat émis par un tribunal ou d'un *subpoena* et dans ce cas avec avis à la personne visée. Ainsi, en ce cas, le maintien de la confidentialité de l'enquête imposera la nécessité de recourir à une demande d'émission d'un mandat de perquisition[66]. L'émission d'un mandat est sujette à la preuve de faits « showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation *».*

En bref, bien que les dispositions du *Electronic Communication Privacy Act* applicables aux fournisseurs de services de télécommunication interdisent à ceux-ci, à titre de règle générale, de divulguer le contenu d'une communication, et de divulguer des informations relatives à cette communication ou relatives à ses clients à toute entité gouvernementale, les dispositions qui prévoient des procédures d'accès et qui accordent des pouvoirs d'enquête ont préséance sur cette interdiction de divulgation.

Or, les informations révélées par Edward Snowden relativement aux programmes de surveillance mis en place par les services de renseignements américains mettent en lumière l'interprétation qui a été faite des dispositions modificatrices du *Patriot Act* par le Tribunal FISA et l'étendue de l'utilisation qui en a vraisemblablement été faite[67].

Ainsi, nous constatons que dans le cadre de programmes appelés PRISM et Tempora (FAIRVIEW/STORMBRE/BLARNEY/OAKSTAR) vraisemblablement mis sur pied en vertu de l'ordre exécutif 12333[68] et d'ordonnances émises par le Tribunal FISA[69], les autorités américaines auraient, avec ou sans la collaboration des agences de renseignements du groupe des *Five Eyes* (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande), recueilli, de façon « accessoire » à leurs enquêtes antiterroristes, d'énormes quantités de métadonnées téléphoniques, de courriels, et d'historiques de navigation, en interceptant les paquets de données directement à même les réseaux de fibres optiques ou en les obtenant des principaux fournisseurs de services Internet et de télécommunications.

L'ampleur des interceptions effectuées est telle qu'indépendamment du fournisseur de services infonuagiques qui pourrait être retenu par une organisation, le programme d'interception des données à même les réseaux de communication est nécessairement susceptible d'entraîner une divulgation et d'affecter le caractère confidentiel de documents confiés et transmis de façon électronique en Amérique du Nord.

Dans le cadre d'une analyse effectuée en vertu de l'article 17 LPRPSP et 70.1 LADOPPRP, il nous apparaît que l'enjeu consiste ultimement à déterminer si une telle divulgation s'inscrit à l'intérieur d'un régime juridique qui reconnaît le principe de la confidentialité des renseignements personnels, et si cela correspond conséquemment à une communication similaire à celle faite « à un organisme chargé en vertu de la loi de prévenir, détecter ou réprimer le crime ou les infractions aux lois, qui le requiert dans l'exercice de ses fonctions, si le renseignement est nécessaire pour la poursuite d'une infraction à une loi applicable au Québec », au sens des articles 59(3) LADOPPRP et 18(3) LPRPSP. Il est important de noter que dans les recommandations publiées au mois de novembre 2013, la commission européenne, dont le critère de reconnaissance d'une sphère de sécurité est celui de la « protection adéquate », référait quant à elle à l'importance que l'exception relative à sécurité nationale ne soit utilisée que dans la mesure où elle est nécessaire et de façon proportionnelle[70].

Pour compléter l'analyse, il est nécessaire d'examiner quels sont les droits qui peuvent être invoqués par les organismes canadiens chargés de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

C. Les droits d'accès accordés aux autorités gouvernementales canadiennes

Dans la foulée des attaques terroristes survenues sur le territoire américain, le parlement canadien a adopté en décembre 2001, la *Loi antiterroriste*[71], ayant pour effet d'entraîner des modifications à plusieurs lois, dont le *Code criminel,* de façon à élargir la portée des pouvoirs accordés aux autorités gouvernementales aux fins de protéger

la sécurité nationale.

Différentes lois canadiennes accordent aujourd'hui des droits d'interception et de saisie aux autorités gouvernementales canadiennes :

- *Code criminel ;*
- *Loi sur le Service canadien du renseignement de sécurité ;*
- *Loi sur la protection de l'information ;*
- *Loi sur la défense nationale ;*
- *Loi sur l'entraide juridique en matière criminelle ;*
- Projet de loi C-30 – *Loi édictant la loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois*[72].

La *Loi sur le Service canadien du renseignement de sécurité* et la *Loi sur la défense nationale* contiennent des dispositions accordant des pouvoirs similaires à ceux accordés par les lois américaines. À titre d'exemple, l'article 21 de la *Loi sur le Service canadien du renseignement de sécurité* qui prévoit la possibilité pour un juge de la Cour fédérale d'émettre, sur demande présentée *ex parte* et à huis clos, un mandat autorisant l'interception de communications, l'obtention d'informations, de documents ou d'objets et à cette fin :

> *a*) l'accès à un lieu ou un objet ou l'ouverture d'un objet ;
>
> *b*) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé ;
>
> *c*) l'installation, l'entretien et l'enlèvement d'objets.

La loi énonce par ailleurs la possibilité pour le juge d'ajouter au mandat les conditions qu'il estime indiquées dans l'intérêt public, ce qui inclut vraisemblablement de façon générale des ordonnances de non-divulgation destinées aux personnes dont la coopération est requise dans le cadre de l'exécution du mandat, tel qu'un fournisseur de télécommunication.

Par ailleurs, la *Loi sur la défense nationale* (art 273.65) prévoit que le ministre de la Défense nationale peut, afin d'obtenir des renseignements étrangers, autoriser le *Centre de la sécurité des télécommunications* à intercepter des communications privées (impliquant des entités étrangères) liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Le ministre peut également autoriser l'interception de communications privées au sens du *Code criminel* afin de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada.

Le *Code criminel* dont les dispositions ont été modifiées par la *Loi antiterroriste* en 2001 (art. 83.01 et suiv.) prévoit la possibilité pour le procureur général de présenter *ex parte* et à huis clos à un juge de la Cour fédérale une demande en vue de l'émission d'un mandat de confiscation en regard de biens appartenant à un groupe terroriste ou susceptibles d'être utilisés pour faciliter une activité terroriste.

Ces deux mécanismes offerts au Service canadien du renseignement et au ministre de la Défense nationale et les procédures qui en encadrent l'exercice sont assimilables aux droits accordés aux autorités américaines en vertu du *Foreign Intelligence Surveillance Act.*

D'autres dispositions du *Code criminel* accordent des droits d'interception de communications (184.4/185), de fouille et de saisie de données (487(2.1)), d'émission d'ordonnance de communication de documents (487.012) et d'assistance (487.02).

De façon générale, l'exercice des pouvoirs d'accès est assujetti à l'obtention d'une autorisation et nécessite une preuve par affidavit de motifs raisonnables indicatifs de la commission, ou d'un risque de commission d'une infraction, une description des démarches d'enquête effectuées et la portée de l'interception ou de la perquisition pour laquelle une autorisation est recherchée.

Il faut finalement souligner que le Canada a adopté une *Loi sur l'entraide juridique en matière criminelle*[73] afin de mettre en oeuvre les engagements souscrits aux termes de traités de coopération judiciaire. En vertu de cette loi, le ministre de la Justice peut autoriser un État étranger et, le cas échéant, l'assister aux fins de présenter une requête de mandat pour fouille, saisie, perquisition, ou obtention d'éléments de preuve. Dans une affaire récente, le procureur général du Canada a demandé et obtenu, pour et au nom du gouvernement des États-Unis, un mandat de saisie visant des serveurs informatiques appartenant à un fournisseur canadien de services infonuagiques (Equinix) qui auraient été utilisés dans le cadre des activités de Megaupload Ltd.[74], laquelle fait l'objet de poursuites aux États-Unis.

La possibilité de telles procédures constitue évidemment un risque négligeable pour la plupart des organisations, mais s'inscrit dans une tendance à l'expansion de la juridiction des autorités gouvernementales, laquelle ne s'arrête pas aux limites territoriales, mais s'étend également aux actifs, installations, systèmes et documents auxquels une entité a accès ou dont elle détient le contrôle, et tend à réduire significativement l'efficacité potentielle d'une restriction géographique contractuelle[75].

Au-delà du libellé des lois accordant des droits d'accès aux autorités gouvernementales, les propos suivants de la Commissaire à l'information et à la protection de la vie privée de l'Ontario sont indicatifs de son appréciation du risque que représente le *Patriot Act* :

> [...] don't let things like the *Patriot Act*... I mean, it's just such a red herring. It's nothing. There are stronger, before the *Patriot Act* existed, there are other things that would do what the *Patriot Act* would suggest that you might be concerned about. Whether you have the *Patriot Act* or not it doesn't matter. There will always be law enforcement methods and techniques that will access certain types of information here, there and everywhere. What you should concern yourself with is the kind of accountability that you will be able to maintain if your e-mail systems go into the cloud. That's what would concern me.[76]

D. Application effective des droits d'accès au Canada

Les données publiques officielles relatives à l'exercice des pouvoirs d'accès accordés aux gouvernements canadien et américain aux termes des lois relatives à la sécurité nationale sont de nature quantitative. Les données publiées ne fournissent aucun éclairage sur les personnes et documents visés, ni sur la nature et l'étendue des enquêtes dans le cadre desquelles des communications et des documents sont interceptés, fouillés ou perquisitionnés. Le rapport annuel publié par le Commissaire du Centre de la sécurité des télécommunications est toutefois instructif en regard des moyens d'enquête à la portée du Commissaire[77].

Nous ne disposons pas actuellement d'informations significatives en regard de l'état des opérations de surveillance au Canada. Certains documents publiés en 2013 sont toutefois indicatifs du degré de collaboration qui existe entre les autorités respectives des pays membres du groupe des « *Five eyes* » (Canada, États-Unis, Grande-Bretagne, Australie et Nouvelle-Zélande). Un document publié par la Société Radio-Canada révèle notamment que le Canada a collaboré à la surveillance des communications au cours de sommets tenus au Canada en 2010[78].

À la lumière de ce qui précède, nous devons constater que l'étendue des pouvoirs accordés par les lois aux autorités canadiennes et américaines est similaire. L'interprétation [79]

qui en est faite peut toutefois être significativement différente .

Il demeure que selon l'information disponible à ce stade-ci et sous réserve du sort des procédures recherchant des déclarations d'inconstitutionnalité des lois en vertu desquelles ils ont été autorisés, les programmes de surveillance déployés par les autorités américaines s'inscrivent dans un ordre juridique qui reconnaît le droit à la vie privée et la confidentialité des renseignements personnels, et qui comporte tout comme le droit canadien des exceptions en regard des droits d'accès accordés aux autorités gouvernementales. En effet, les différentes opérations de surveillance ont été autorisées et menées en vertu, selon le cas, de pouvoirs accordés par la loi (*National Security Letters du* FBI), un ordre de l'exécutif (Executive Order 12333) ou des ordonnances rendues par le Tribunal FISA en vertu du *Foreign Intelligence Surveillance Act.*

Dans le cadre d'un processus décisionnel effectué en tenant compte des articles 17 LPRPSP et 70.1 LADOPPRP, une organisation pourrait selon nous validement conclure que les documents confiés à un prestataire de services en mode infonuagique soumis à la juridiction américaine bénéficieront néanmoins d'une protection équivalente à celle prévue par les lois québécoises qui prévoient également des exceptions à l'interdiction de communication sans consentement en faveur d'un organisme chargé de prévenir, détecter ou réprimer les crimes, lesquels disposent de pouvoir et de mécanismes qui, sous réserve des *National Security Letters* émises par le FBI, sont assimilables aux prérogatives des autorités américaines.

Les révélations relatives au programme de surveillance appelé Tempora (FAIRVIEW/STORMBRE, BLARNEY/OAKSTAR) par lequel les autorités britanniques et américaines recueilleraient les paquets de données à même les flux des câbles optiques transitant par leurs territoires démontrent que les frontières du Québec ou du Canada ne représentent pas un rempart significatif contre la surveillance effectuée par d'autres gouvernements.

Ces révélations tendent à démontrer que c'est au moment où l'opportunité de recourir à des services en mode infonuagique est considérée que le risque d'accès par un gouvernement étranger doit être analysé, et ce, indépendamment de l'existence d'un lien de rattachement du fournisseur avec les États-Unis ou de la localisation de ses installations.

Cette réalité milite pour une analyse exhaustive de la sensibilité des documents susceptibles d'être confiés et des mécanismes de sécurité à la disposition des organisations. L'analyse de la légalité n'écarte évidemment pas la nécessité de considérer l'opportunité de recourir à des services en mode infonuagique en procédant à une analyse de risque en bonne et due forme. Comme en toutes circonstances, les organisations devraient s'attarder à déterminer le degré de sensibilité des catégories de documents visés par une offre de services infonuagiques, au profil des fournisseurs de services, ainsi qu'aux mesures de sécurité susceptibles d'être appliquées[80]. C'est notamment le processus qui a été suivi par le gouvernement canadien en 2004 et 2005 en regard des contrats d'impartition des institutions gouvernementales[81].

Conformément aux obligations imposées par la loi et au principe de transparence, les organisations doivent dénoncer leur recours aux services de tiers et préciser que les renseignements personnels qui leur sont confiés sont susceptibles d'être conservés dans d'autres juridictions et par le fait même sujets aux droits d'accès des gouvernements de ces juridictions. Afin d'être en mesure de fournir un avis qui soit intelligible, une organisation devra se conformer aux exigences de l'article 26 de la LCCJTI en dénonçant à son fournisseur le caractère confidentiel des documents confiés, exiger des précisions et des engagements en regard du *situs* des installations, et convenir des mesures de sécurité. Un tel exercice de vérification devra aussi s'étendre au recours du fournisseur à d'autres prestataires de services, d'infrastructures ou de services, ce qui est fréquent dans les modèles d'affaires des fournisseurs de services en technologies de l'information.

Bien que les conditions d'utilisation des fournisseurs de services grand public soient des contrats d'adhésion, les fournisseurs qui s'adressent aux entreprises et organisations gouvernementales sont plus que jamais sensibilisés à l'importance des enjeux liés à la protection des renseignements personnels pour leurs clients et démontrent désormais une volonté d'adapter leurs offres de façon à offrir plus de transparence à leurs clients[82].

---

* M^e Jean-François De Rico, B.A. (philosophie), LL.B., avocat, associé Langlois Kronström Desjardins s.e.n.c.r.l., membre de LEXING.

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud computing synopsis and recommendations*, Special publication 800-146, 2012. Sur les caractéristiques et les modèles d'offres de services, voir aussi : CLOUD SECURITY ALLIANCE, *Security Guidance for Critical Areas of Focus in Cloud Computing*, v. 3.0, CSA, 2011.

2. GARTNER, *Forecast: Consumer Digital Storage Needs – Press Release, 2010-2016* [http://www.gartner.com/newsroom/id/2060215] (consulté le 23 décembre 2013).

3. INTERNET SOCIETY, *Un bref historique de l'Internet* [http://tinyurl.com/kr4ejww] (consulté le 2 janvier 2014) ; COMPUTER HISTORY MUSEUM, *Internet History* [http://www.computerhistory.org/internet_history/] (consulté le 2 janvier 2014) ; voir aussi Thomas GREENE, Larry James LANDWEBER et Georges STRAWN, *A Brief History of NSF and the Internet* [http://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm] (consulté le 2 janvier 2014). Pour des études approfondies, voir Janet ABBATE, Inventing the Internet, MIT Press, 1999 ; Matthew LYON et Kathie HAFNER, *Where wizards stay up late – The Origins of the Internet*, Simon & Schuster, 1998.

4. L'apparition de ce type d'offres de services commerciales, dont Amazon Web Services – EC2, remonte au milieu des années 2000.

5. Pour une analyse comparative des conditions d'utilisation de différents fournisseurs, voir : Simon BRADSHAW, Christopher MILLARD et Ian WALDEN, « Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of cloud computing services », (2011) 19 *International Journal of Law and Information Technology* 187.

6. Notons que les premières révélations sur les opérations de surveillance remontent au mois de décembre 2005 (http://www.pulitzer.org/archives/7037) (consulté le 6 janvier 2014).

7. Sur les révélations d'Edward Snowden et les programmes de surveillance mis au jour, voir l'excellent site élaboré par *The Guardian* http://tinyurl.com/nv8dbgu (consulté le 5 janvier 2014) ; voir aussi le site de l'Electronic Frontier Foundation : https://www.eff.org/nsa-spying.

8. *Klayman* v. *Obama*, 13 Civ. 0851 (US DC), 16 décembre 2013 (legaltimes.typepad.com/files/obamansa.pdf) ; *ACLU* v. *Clapper*, 13 Civ. 3994 (US SDNY), 27 décembre 2013 (https://www.aclu.org/national-security/aclu-v-clapper-legal-documents).

9. La *Charte canadienne des droits et libertés* (art. 8), la *Charte des droits et libertés de la personne* du Québec (art. 4, 5, 6, 7) et le *Code civil du Québec* (art. 35) reconnaissent le caractère fondamental du droit à la vie privée.

10. RLRQ, c. C-1.1.

11. RLRQ, c. A-2.1.

12. RLRQ, c. P-39.1.

13. Le *Décret d'exclusion visant des organisations de la province de Québec* (DORS/2003-374) adopté en vertu de l'article 26(2)b) de la LPRPDE écarte l'application de la partie 1 de la LPRPDE « à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels qui s'effectuent à l'intérieur de la province de Québec ». Dans les *Lignes directrices sur le traitement transfrontalier des données personnelles,* le Commissariat à la protection de la vie privée du Canada mentionne expressément « les organisations dont les activités commerciales dans une province ne sont pas assujetties à la LPRPDE doivent savoir que les transferts transfrontaliers le sont ».

14. Sur la LCCJTI, voir notamment le site www.lccjti.ca et Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville,

Éditions Yvon Blais, 2012.

15. Pour une analyse complète des dispositions relatives à la transmission, voir : Patrick GINGRAS et Jean-François DE RICO, « La transmission des documents technologiques », dans *Actes de la XX^e conférence des juristes de l'État*, Cowansville, Éditions Yvon Blais, 2013, p. 409.

16. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, art. 5 et annexe I, principe 4.1.3.

17. *Deschesnes* c. *Groupe Jean Coutu*, [2000] CAI 216, EYB 2000-178499.

18. Pour une analyse des notions de « communication », « détention », « hébergement », « conservation » et « contrôle », voir Nicolas VERMEYS et al., *Les balises juridiques de l'infonuagique : sécurité, vie privée et propriété intellectuelle* (titre provisoire), (en préparation) ; Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Thémis, 2010, p. 93-157.

19. Ces thèses ont notamment été invoquées par les auteurs Raymond DORAY et François CHARRETTE, *Accès à l'information*, Cowansville, Éditions Yvon Blais, 2013 (mise à jour), p. III/ 70.1-1, ainsi que par Karl DELWAIDE, *Data transfers rules in Quebec*, Bulletin Fasken Martineau, mai 2010 ; voir aussi par le même auteur, *Cent fois sur le métier... l'impartition de services à l'étranger : résumé des conclusions d'enquête en vertu de la LPRPDÉ*, n° 394, Bulletin Fasken Martineau, décembre 2008.

20. *Décret d'exclusion visant des organisations de la province de Québec*, DORS/2003-374, le processus et les critères généraux d'appréciation sont décrits dans *Processus de détermination du caractère* comme « essentiellement similaire » d'une loi provinciale par le gouverneur en conseil, Gazette du Canada, vol. 136, n° 31 – Le 3 août 2002 (à la page 2385).

21. Dans les lignes directrices sur le traitement transfrontalier des données personnelles, le Commissariat à la protection de la vie privée du Canada écrit : « La LPRPDE n'interdit pas aux organisations du Canada de transférer des renseignements personnels à une organisation dans un pays étranger aux fins de traitement. Toutefois, en vertu de la LPRPDE, les organisations sont tenues responsables de la protection des transferts de renseignements personnels en vertu de chaque accord d'impartition individuel. Le Commissariat à la protection de la vie privée du Canada peut enquêter sur des plaintes et mener des vérifications concernant les pratiques de traitement des renseignements personnels des organisations ».

22. Henri BRUN, Guy TREMBLAY et Eugénie BROUILLET, Droit constitutionnel, 5^e éd., Cowansville, Éditions Yvon Blais, 2008, p. 456. Pour une application des principes dans un autre contexte, voir Nicolas VERMEYS, « C-11, le cadre juridique des technologies de l'Information et la responsabilité des intermédiaires techniques québécois : une dualité de régime (in)utile(s) ? », (2013) 25 *C.P.I.* 1053, 1075.

23. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur le traitement transfrontalier des données personnelles*, CPVPC, 2009.

24. BUREAU DU SURINTENDANT DES INSTITUTIONS FINANCIÈRES, *Lignes directrices sur l'impartition d'activités, de fonctions et de méthodes commerciales (B-10)*, 2009 (http://www.osfi-bsif.gc.ca/Fra/Docs/b10_Sound.pdf).

25. L.C. 1991, c. 46.

26. BUREAU DU SURINTENDANT DES INSTITUTIONS FINANCIÈRES, *id.*, n° 7.1.

27. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur le traitement transfrontalier des données personnelles*, CPVPC, 2009.

28. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels*, Juillet 2010 (http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eerpr-fra.asp?format=print).

29. L.Q. 2006, c. 22.

30. ASSEMBLÉE NATIONALE DU QUÉBEC, 37^e législature, 2^e session, Journal des débats de la Commission de la culture, Étude détaillée du projet de loi n° 86 – *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, mercredi 31 mai 2006, vol. 39, n° 18. Un auteur ayant participé à la rédaction du projet de loi et aux débats parlementaires à titre d'avocat du ministère de la Justice a par ailleurs indiqué à la suite de l'adoption de la loi que l'article 70.1 avait été adopté « dans la foulée notamment de certaines préoccupations soulevées par l'adoption aux États-Unis de la *USA Patriot Act* qui facilite la transmission de renseignements personnels au FBI », voir Yves D. DUSSAULT, *Modifications au régime de protection des renseignements personnels*, texte présenté lors du Colloque du Barreau du Québec, novembre 2006 (http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/modifications-prp.pdf).

31. Pour une analyse parvenant à l'opinion contraire, voir Nicolas VERMEYS et al., *Les balises juridiques de l'infonuagique : sécurité, vie privée et propriété intellectuelle* (titre provisoire), (en préparation).

32. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur le traitement transfrontalier des données personnelles*, CPVPC, 2009 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Tracer le chemin – Principaux développements au cours des sept premières années d'application de la LPRPDE*, 2008. Voir aussi les conclusions du Commissaire dans les enquêtes 313, 333, 365 et 394 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information : La protection de la vie privée et l'externalisation* (secteur privé)/(secteur public), Janvier 2014 (http://www.priv.gc.ca/resource/fs-fi/02_05_d_57_os_f.asp).

33. Kris KLEIN, Clarification de l'application du droit canadien de la protection des renseignements personnels au transfert transfrontalier de ces renseignements du Canada vers les États-Unis, 2009 (http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/fra/gv00508.html) ; Karl DELWAIDE, *Data transfers rules in Quebec*, Bulletin Fasken Martineau, mai 2010 ; voir aussi par le même auteur, *Cent fois sur le métier... l'impartition de services à l'étranger : résumé des conclusions d'enquête en vertu de la LPRPDÉ*, n° 394, Bulletin Fasken Martineau, décembre 2008.

34. L'article 8(3) de la LPRPSP impose l'obligation d'informer la personne concernée au moment où elle constitue un dossier « de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification ». Nous sommes d'avis que l'objectif de cette disposition était de permettre un exercice effectif du droit d'accès et de rectification des renseignements conservés dans un dossier physique, et que cette disposition devrait être revue en fonction des dossiers dématérialisés.

35. Art. 67.3 LADOPPRP et 4(6) du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, r. 2.

36. Constitution des États-Unis, IV amendement : « The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized ».

37. Daniel J. SOLOVE, « A Taxonomy of Privacy », (2006) 154 *U. of Penn.* L. R. 477 ; MORRISON & FOERSTER, « Privacy Library », <http://www.mofo.com/privacylibrary/PrivacyLibraryLanding.aspx?xpST=PrivacyLibraryLanding> ; DEPARTMENT OF COMMERCE (U.S.A.), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, 2010, p. 9.

38. *United States* v. *Miller*, 425 U.S. 435 (1976) ; *Smith* v. *Maryland*, 442 U.S. 735 (1979). Dans *U.S.* v. *Warshak*, 631 F.3d 266 (6th Cir. 2010), une cour d'appel fédérale a toutefois distingué ce précédent et conclu en regard de courriels : « Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP." Warshak I, 490 F.3d at 473 ; see Forrester, 512 F.3d at 511 (suggesting that "[t]he contents [of email messages] may deserve Fourth Amendment protection"). The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional ». Ces mêmes précédents ont également été écartés par une cour fédérale dans une décision récente : *Klayman* v. *Obama*, 13 Civ. 0851 (US DC), 16 déc. 2013. Pour une analyse de l'application de la protection constitutionnelle aux documents conservés en mode infonuagique, voir : David A. COUILLARD, « Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Expectations in Cloud Computing » (2009) 93 *Minnesota Law Rev.* 2205.

39. Samuel WARREN et Louis BRANDEIS, « The Right to Privacy », (1890) 4 *Harvard Law Review* 193 ; William L. PROSSER, « Privacy », (1960) 48 *California Law Review* 383 ; *Mainstream Marketing Services. Inc. v. FTC*, 358 F.3d 1228, 1232-33 (10th Cir. 2004).

40. U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, *Secretary's Advisory Committee on Automated Personal Data Systems, Records*, Computers, and the Rights of Citizens (July 1973).

41. http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm.

42. Privacy Act of 1974, 5 U.S.C. § 552a.

43. OFFICE OF MANAGEMENT AND BUDGET, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28, 948 (Nov. 21, 1975).

44. *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) ; *Gramm-Leach-Bliley Act* of 1999 (GLBA) ; *Family Educational Rights and Privacy Act* of 1974 (FERPA) ; *Children's Online Privacy Protection Act* of 1998 (COPPA) ; *Fair Credit Reporting Act* of 1970 ; *Right to Financial Privacy Act* of 1978 ; *Electronic Communications Privacy Act* of 1986.

45. Pour consulter les différentes lois étatiques, voir : MORRISON & FOERSTER, « Privacy Library », <http://www.mofo.com/privacylibrary/PrivacyLibraryLanding.aspx?xpST=PrivacyLibraryLanding> (consultée le 20 décembre 2013).

46. La Loi est constituée du *Wiretap Act* du *Stored Communications Act* et du *Pen Register Act.* La portée de la Loi a fait l'objet d'interprétations divergentes et le libellé utilisé en 1986 mériterait d'être revisité afin d'en clarifier la portée et de permettre une interprétation qui puisse suivre l'évolution technologique.

47. *Warshak* v. *United States*, 532 F.3d 521 (6th Cir. 2008).

48. *United States* v. *Warshak*, 631 F.3d 266 (6th Cir. 2010).

49. Au sujet de cette loi, voir : U.S. INTERNET SERVICE PROVIDER ASSOCIATION, « Electronic Evidence Compliance – A Guide for Internet Service Providers », (2003) 18 *Berkeley Tech. L.J.* 945.

50. Notamment en regard de la durée de conservation et de l'impact d'une conservation dépassant 180 jours.

51. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur le traitement transfrontalier des données personnelles*, CPVPC, 2009 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Tracer le chemin – Principaux développements au cours des sept premières années d'application de la LPRPDE*, 2008. Voir aussi les conclusions du Commissaire dans les enquêtes 313, 333, 365 et 394 ainsi que COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information : La protection de la vie privée et l'externalisation (secteur privé)/(secteur public)*, janvier 2014 (http://www.priv.gc.ca/resource/fs-fi/02_05_d_57_os_f.asp).

52. *OPINION 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, janvier 1999.

53. 2000/520/CE : Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité ».

54. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

55. Annexe I de la Décision de la Commission du 26 juillet 2000 ; *Principes de la « sphère de sécurité » relatifs à la protection de la vie privée publiés par le ministère américain du Commerce*, le 21 juillet 2000.

56. COMMISSION EUROPÉENNE, MEMO/13/1059 27/11/2013, *Restoring Trust in EU-US data flows – Frequently Asked Questions*, novembre 2013.

57. Public Law 107– 56– OCT. 26, 2001 (http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf).

58. RSBC 1996, c.165.

59. Francoise GILBERT, *What rules regulate government access to Data held by us cloud service providers*, Cloud Security Alliance Whitepaper, février 2013. Voir aussi : Hogan LOVELLS, *A Global Reality: Governmental Access to Data in the Cloud. A comparative analysis of ten international jurisdictions*, 2012.

60. Le *Foreign Intelligence Surveillance Act* a de nouveau été modifié par le *Protect America Act* en 2007 et le *Foreign Intelligence Surveillance Amendments Act* en 2008 à la suite de la mise au jour du programme de surveillance des communications de citoyens américains autorisé par l'administration du président Bush.

61. Pour les rapports du procureur général sur les demandes adressées au Tribunal FISA en 2011 : http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf et https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

62. Andrew E. NIELAND, « National Security Letters And The Amended Patriot Act », (2007) 92 *Cornell L. Rev.* 1201.

63. *In re National Security Letters*, No. C 11-02173 SI (N.D. Cal. March 15, 2013) en appel : U.S. Court of Appeals 9th Circuit Case Nos. 13-15957, 13-16731 and 13-16732, (http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000715) (consulté le 7 janvier 2014). Voir aussi *ohn Doe, Inc.* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008).

64. http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf et https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

65. 18 USC CHAPTER 121, sec. 2701-2711 http://uscode.house.gov/download/pls/18C121.txt.

66. Des rapports annuels faisant état des mandats émis sont par ailleurs publiés par l'administration chapeautant les tribunaux fédéraux américains : http://www.uscourts.gov/Statistics/WiretapReports.aspx.

67. Sur les révélations d'Edward Snowden et les programmes de surveillance mis au jour, voir l'excellent site élaboré par *The Guardian* http://tinyurl.com/nv8dbgu (consulté le 5 janvier 2014).

68. Executive Order 12333, United States Intelligence Activities (https://www.cia.gov/about-cia/eo12333.html).

69. Un exemple d'ordonnance visant la communication des métadonnées de tous les appels téléphoniques impliquant un interlocuteur aux États-Unis destiné à la société de télécommunication Verizon est disponible à http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/1.

70. COMMISSION EUROPÉENNE, MEMO/13/1059 27/11/2013, *Restoring Trust in EU-US data flows – Frequently Asked Questions*, novembre 2013.

71. *Loi modifiant le Code criminel, la Loi sur les secrets officiels, la Loi sur la preuve au Canada, la Loi sur le recyclage des produits de la criminalité et d'autres lois, et édictant des mesures à l'égard de l'enregistrement des organismes de bienfaisance, en vue de combattre le terrorisme*, L.C. 2001, c. 41 (la « Loi antiterroriste »).

72. Quant au projet de loi C-30 visant à introduire des dispositions relatives à « l'accès légal », soit l'interception de communications privées et la saisie d'information par les organismes chargés de la sécurité nationale ou du contrôle d'application des lois, et ce, sans nécessité d'autorisation judiciaire, le gouvernement a décidé de ne pas en poursuivre l'étude et de le laisser mourir au feuilleton de la Chambre des communes.

73. L.R.C. (1985), c. 30 (4^{e} suppl.).

74. *Megaupload Inc.* v. *Attorney General of Canada*, 2012 ONSC 6331 ; *Canada (United States of America)* v. *Equinix Inc.*, 2013 ONSC 193 (CanLII). La saisie a été effectuée en janvier 2012 et la plus récente décision fait état du débat qui a cours sur l'étendue des données qui devront être communiquées.

75. *eBay Canada Limited* c. *Canada (Revenu national)*, 2007 CF 930 (conf. par la CAF) ; *In Re Grand Jury Proceedings – United States of America* v. *The Bank of Nova Scotia*, U.S. CA 11th Cir. 740 F.2d 817.

76. Propos de la Dre Ann Cavoukian relatés par Dan Michaluk sur Slaw <http://www.slaw.ca/2011/02/26/commissioner-cavoukian-says-the-patriot-act-is-nothing/>.

77. COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS – Hon. Robert Décary, *Rapport Annuel 2012-2013*, (http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_f.pdf) (consulté le 3 janvier 2014).

78. Greg WESTON, Glen GREENWALD et Ryan GALLAGHER, *New Snowden docs show U.S. spied during G20 in Toronto*, 27 novembre 2013 (http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448). Le document : http://www.cbc.ca/news2/pdf/summit-doc.pdf (consulté le 3 janvier 2014).

79. Le 17 janvier 2014, le président des États-Unis a publié une directive annonçant une volonté de revoir l'encadrement des pouvoirs de surveillance afin d'assurer une meilleure protection de la vie privée : <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

80. Voir notamment CLOUD SECURITY ALLIANCE, *Security Guidance for Critical Areas of Focus in Cloud Computing*, v. 3.0, CSA, 2011 ; EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), *Cloud computing – Benefits, risks and recommendations for information security*, ENISA, novembre 2009.

81. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Protéger les renseignements personnels – un impératif*, 2006, p. 18.

82. Un groupe de huit entreprises américaines d'envergure internationale s'est récemment joint aux voix qui réclament une réforme des lois relatives aux droits d'accès des gouvernements (http://reformgovernmentsurveillance.com/).

Date de dépôt : 5 février 2014