Commissariat à la protection de la vie privée du Canada
Office of the Privacy Commissioner of Canada

Le droit fondamental à la vie privée dans le contexte d'une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre

Mémoire du Commissariat à la protection de la vie privée du Canada dans le cadre de la consultation publique du Groupe de travail par-delà la frontière du gouvernement du Canada

Juin 2011

Table des matières

Introduction

Le Commissariat à la protection de la vie privée du Canada (CPVP) comprend l'importance de faciliter le commerce et d'assurer la sécurité à la frontière. Tout examen des mesures ou nouvelles initiatives visant à abolir certains des obstacles et des retards actuellement vécus par de nombreux voyageurs seraient les bienvenus. Les citoyens canadiens semblent largement appuyer les efforts en vue de limiter les contrôles pénibles et d'améliorer les mesures de sécurité, tout en facilitant les voyages et le commerce transfrontaliers[1].

Parallèlement, il est évident que la déclaration *Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre* (ci-après la Déclaration) vise une approche intégrée de l'évaluation des menaces dans un objectif de sécurité collective[2]. Ce programme serait fondé sur un vaste échange des renseignements personnels des citoyens canadiens. Au cours de la dernière décennie, les contrôles frontaliers et les autres mesures de sécurité mises en place à l'échelle nationale et internationale ont eu de vastes répercussions sur le respect de la vie privée.

Bien que la sécurité des déplacements et des collectivités soit un objectif important tant pour les États-Unis que pour le Canada, il doit être atteint en respectant les libertés fondamentales et le droit à la vie privée. Historiquement, ces valeurs et ces principes ont constitué les piliers des sociétés ouvertes et démocratiques que nos deux pays ont bâties ensemble. L'importance de ces engagements perdure encore aujourd'hui : la protection des renseignements personnels et le respect de la vie privée des personnes doivent demeurer au centre des préoccupations, peu importe le contexte (poste frontalier ou aéroport, billetterie ou ordinateur personnel).

Pour nos commentaires sur la Déclaration et les programmes pouvant en découler, nous avons organisé nos points de vue en fonction des thèmes présentés à la fois dans le document officiel, mais aussi dans le document de référence du Commissariat intitulé *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*[3]. Nous avons préparé des observations générales ainsi que des recommandations spécifiques à prendre en considération sur les thèmes suivants :

- contrôles frontaliers généraux et mesures de sécurité;
- mécanismes d'échange de renseignements, de surveillance et de recours;
- utilisation de la biométrie;
- mise en place d'un système continental d'entrée et de sortie;
- cybersécurité et renseignements personnels;
- protection de la vie privée dans les interventions sanitaires d'urgence.

---

[1] Nik Nanos, « Canadiens et Américains ne voient aucune contradiction entre sécurité frontalière, partenariat économique et leurs intérêts nationaux », *Options politiques* (mars 2011), URL : http://www.irpp.org/po/archive/mar11/nanos_f.pdf.

[2] Gouvernement du Canada, *Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre. Déclaration du Premier ministre du Canada et du Président des États-Unis d'Amérique* (4 février 2011), URL : http://www.borderactionplan-plandactionfrontalier.gc.ca/psec-scep/declaration-declaration.aspx?lang=fra.

[3] Commissariat à la protection de la vie privée du Canada, *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité du 21e siècle* (2010), URL : http://www.priv.gc.ca/information/pub/gd_sec_201011_f.cfm.

Nous avons également inclus en annexe la correspondance antérieure entre le Commissariat et le Groupe de travail par-delà la frontière (GTPF) sur l'importance de tenir compte des normes de protection des données personnelles internationalement reconnues au moment de la conception du programme[4].

Contrôles frontaliers généraux et mesures de sécurité

Les expériences vécues par de nombreux voyageurs canadiens au cours des dernières années aux postes frontaliers et dans les aéroports démontrent leurs inquiétudes persistantes à l'égard de la protection de la vie privée lors des déplacements[5]. Le Commissariat à la protection de la vie privée du Canada reçoit continuellement des demandes de renseignements des médias, de la population et des élus concernant des incidents survenus lors de déplacements[6], notamment dans les cas où les personnes ont été retardées, détenues ou se sont vu refuser l'entrée en raison d'expériences documentées remontant à plusieurs années, voire des décennies.

En 2005, de nombreuses personnes résidant au Canada qui avaient préalablement voyagé librement entre le Canada et les États-Unis ont commencé à signaler des difficultés (ou des refus d'entrée) alors qu'ils tentaient de traverser la frontière par affaires, pour faire des achats ou pour visiter des amis et de la famille. Ce changement découle des nouveaux pouvoirs qui permettent aux agents du service américain des douanes et de protection des frontières (CBP) d'utiliser les renseignements de diverses sources publiques et de services de renseignement privés afin d'accroître la vérification des antécédents des personnes qui tentent d'entrer au pays[7]. Les agents du CBP peuvent effectuer des contrôles non seulement à l'aide des systèmes conçus pour les mandats ou avis de signalement en vigueur, mais aussi à l'aide d'information générale et accessible au public sur les voyages, les études et les nouvelles, entre autres.

La vie privée peut se définir comme le droit du particulier de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant.
~ R. c. Duarte, [1990] 1 R.C.S. 30

Au Canada, de nombreux effets secondaires de la collecte, de l'analyse et de l'échange de renseignements personnels à grande échelle avec les organismes de sécurité et les autorités

[4] Conférence internationale des commissaires à la protection des données et de la vie privée, *Normes internationales sur la vie privée et la protection des données personnelles* (Madrid, 2009), URL : http://www.privacyconference2009.org/dpas_space/Resolucion/common/resolution_international_standards_fr.pdf.
[5] Pour un bref compte rendu sur ces préoccupations, consulter : Coaliation pour la surveillance des libertés civiles, *Rapport de recherche sur les contrôles frontaliers et les atteintes à la liberté et aux droits des voyageurs* (2010), URL : http://surveillancedesvoyageurs.ca/updir/travelwatchlist/Rapport_listes_de_surveillance.pdf.
[6] Commissariat à la protection de la vie privée du Canada, *À l'enregistrement : Votre droit à la vie privée dans les aéroports et aux postes frontaliers* (février 2010), URL : http://www.priv.gc.ca/fs-fi/02_05_d_45_f.cfm.
[7] *Intelligence Reform and Terrorism Prevention Act of 2004* (Pub. L. 108-458, 118, Stat. 3638), Title V: Border protection, immigration, and visa matters / Sub: Advanced Technology Northern Border Security Pilot Program, section 5102; voir également département de la Justice des États-Unis, « Federal Statutes Relevant in the Information Sharing Environment (ISE) » (2010), URL : http://www.it.ojp.gov/default.aspx?area=privacy&page=1282 et Krista Boa et autres « Can ID? Visions for Canada's Identity Policy », rapport conjoint de l'Université de Toronto et de la London School of Economics (2006), URL: http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/can_id_report.pdf.

frontalières des États-Unis n'ont manifestement pas été prévus. Les incidents relevés vont de l'inconvénient d'être intercepté à un passage frontalier en raison d'une tentative de suicide commise cinq ans auparavant à l'extradition tragique d'un citoyen canadien vers la torture en Syrie[8]. Au moment où le Canada et les États-Unis négocient en vue d'une simplification des procédures frontalières et des mesures de sécurité, ces expériences doivent être prises en considération.

La Déclaration signée plus tôt cette année ajoute un poids considérable à l'importance de la protection des droits de la personne, des libertés civiles et de la vie privée. L'objectif de l'analyse et des recommandations suivantes est de s'assurer que les deux gouvernements respectent cet engagement.

Recommandations du CPVP

1. La transparence et l'ouverture permanentes des deux gouvernements sont essentielles : Les dispositifs de balayage corporel, le ciblage automatisé fondé sur l'information préalable sur les voyageurs et les dossiers passagers (IPV et DP), le profilage racial, religieux et linguistique, les collectes de données biométriques et le dépistage fondé sur les comportements sont des pratiques controversées aux États-Unis et au Canada. Puisque la technologie facilite l'utilisation de pratiques invasives, il importe de mettre en place des mécanismes de plainte et une reddition de comptes claire des deux côtés de la frontière. De plus, la pertinence des mesures doit être revue de manière ouverte et continue. Toute nouvelle exigence devrait être accompagnée d'explications claires à l'intention du public démontrant la nécessité, les contrôles et les recours.

2. Les normes juridiques et les seuils les plus élevés doivent être observés dans une mise en application intergouvernementale : L'adhésion à des principes de protection de la vie privée déterminés et clairement articulés, respectés par les deux parties, sera essentielle pour l'application transfrontalière de la loi. Lorsque la surveillance et d'autres méthodes d'enquête sont employées, les règles d'engagement et les autorisations doivent s'accompagner des niveaux les plus élevés de protection adéquate. Les représentants des gouvernements devraient résister à la tentation de réduire les normes de protection de la vie privée.

3. Une évaluation des facteurs relatifs à la vie privée et des autorisations législatives sans équivoque sont nécessaires pour toutes les mesures connexes : Toute mesure de sécurité concertée fondée sur *l'analyse et l'échange* de renseignements personnels de nature délicate devrait être assujettie à une évaluation complète des facteurs relatifs à la vie privée (EFVP). À l'échelle nationale, les programmes doivent être soutenus par les normes constitutionnelles canadiennes et les autorisations législatives fédérales régissant l'application des lois et les pouvoirs en matière de sécurité nationale. Toute mesure de sécurité fondée sur une *collecte conjointe* (en l'absence d'une entente sur l'échange de renseignements) doit être assujettie à des mesures de contrôle et à une surveillance accrues.

---

[8] Isabel Teotonio, « Canadian woman denied entry to U.S. because of suicide attempt » *Toronto Star* (29 janvier 2011), URL : http://www.thestar.com/news/article/930110--canadian-woman-denied-entry-to-u-s-because-of-suicide-attempt; Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Rapport sur les événements concernant Maher Arar* (2006).

4. Concevoir de la formation : Le Canada et les États-Unis devraient examiner sérieusement leur manière de former et d'échanger les employés. La formation professionnelle internationale du personnel des services frontaliers travaillant en première ligne peut être aussi importante à long terme que les échanges de données ou l'évaluation des menaces de routine. Il est capital que les unités frontalières et les agents de contrôle comprennent le cadre légal et le contexte général du Canada et des États-Unis. Les normes professionnelles et la formation sont des contrôles importants et devraient par conséquent tenir compte des initiatives d'échange de renseignements et être une *condition préalable* à l'accès.

5. Promouvoir l'investissement américain dans la surveillance de la protection de la vie privée : En mettant sur pied le US Privacy and Civil Liberties Oversight Board, la Maison-Blanche a créé et commencé à doter un bureau idéal et autonome du gouvernement afin de réfléchir à tout problème ou incident lié à une augmentation des mesures de contrôle de la sécurité[9]. C'est encourageant et nous espérons que cette question demeurera parmi les priorités.

Mécanismes d'échange de renseignements, de surveillance et de recours

Au cours de la dernière décennie, depuis les attentats terroristes de septembre 2001, les gouvernements se sont continuellement demandé si leurs organismes de renseignement et de sécurité devaient échanger des renseignements, et dans quelle mesure, et quelles conditions ou mesures de contrôle devraient encadrer de tels transferts. Au Canada, trois vastes commissions d'enquête menées par les juges O'Connor (2006), Iacobucci (2008) et Major (2010) se sont penchées sur ces questions et ont chacune mené à la production de conclusions et de recommandations relativement aux risques et à la nécessité de la surveillance de l'échange de renseignements[10]. La vérificatrice générale du Canada a également cerné la question de l'échange de renseignements comme étant essentielle pour la confiance du public envers les institutions gouvernementales[11].

D'abord, l'enquête O'Connor s'est attardée aux circonstances de l'enquête sur Maher Arar, à sa détention et à son extradition subséquente en Syrie. Dans son examen de l'enquête, le juge O'Connor a trouvé que les enquêteurs de la Gendarmerie royale du Canada (GRC) ont trop rapidement présumé qu'il y avait « culpabilité par association ». Pire encore, à la suite des attentats survenus aux États-Unis en 2001, la GRC a essentiellement fourni aux autorités

---

[9] Harold Relyea, *Privacy and Civil Liberties Oversight Board: 109th Congress Proposed Refinements* (2005), URL : http://fpc.state.gov/documents/organization/46403.pdf.

[10] Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (2006), URL : http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/fr/index.htm; Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (2008), URL : http://dsp-psd.tpsgc.gc.ca/collection_2010/bcp-pco/CP32-90-1-2010-fra.pdf; Vol 182 d'Air India : Une tragédie canadienne (2010), URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/air_india-ef/final_report-ef/fr/reports/finalreport/index.asp.

[11] Bureau du vérificateur général du Canada, « La sécurité nationale : l'échange de renseignements et d'information » du rapport *Le Point*, mars 2009, URL : http://www.oag-bvg.gc.ca/internet/Francais/parl_oag_200903_01_f_32288.html.

américaines un accès illimité à ses dossiers d'enquête dans le domaine du contre-terrorisme. Les agents de lutte au terrorisme du Federal Bureau of Investigation (FBI) ont eu accès à une copie électronique complète d'une base de données de la GRC contenant des détails sur ses pistes et sur les personnes d'intérêt.

Ces renseignements ont été partagés sans mesures de contrôle ou mises en garde, et c'est à partir de cette information que les responsables américains ont intercepté Maher Arar alors qu'il était dans l'État de New York, en route vers le Canada. En fait, l'importance capitale des contraintes, des mesures de contrôle et des mises en garde pour l'échange de renseignements entre les États-Unis et le Canada est l'une des observations de l'enquête qui a eu le plus d'écho. Les deux gouvernements devraient tenir compte des recommandations importantes du juge O'Connor au moment de déterminer les limites de tous les mécanismes d'échange de renseignements qui pourraient voir le jour à la suite de la Déclaration.

Il y a eu ensuite la commission Iacobucci concernant l'enquête et le traitement de trois autres « personnes d'intérêt » du Canada ayant de possibles liens avec le terrorisme. Dans ce cas, comme dans celui de M. Arar, les personnes ont finalement été renvoyées du Canada et assujetties à des conditions et à un traitement difficiles au cours de leur emprisonnement à l'étranger. L'observation principale qui se dégage de l'examen de ces cas a trait à la sensibilité dont doivent faire preuve les enquêteurs avant d'apposer à des citoyens l'étiquette de « terroriste » ou d'« extrémiste » en raison des conséquences à long terme sur le profil de ces personnes. Maher Arar demeure à ce jour sur la liste de personnes interdites de vols aux États-Unis bien qu'il ait été disculpé de tout blâme au Canada.

Dans un contexte de sécurité tendu aux postes frontaliers, des cas de profilage imprudent ou de dossiers d'enquête mal justifiés peuvent placer des personnes dans des situations véritablement risquées. L'observation la plus remarquée du rapport final du juge Iacobucci a trait au fait que les enquêteurs canadiens du contre-terrorisme n'ont pas su voir la gravité de leurs jugements rapides et qu'ils devront faire preuve de beaucoup plus de prudence dans le futur. Le Commissariat espère que les conclusions de l'enquête Iacobucci seront prises au sérieux dans le cadre des activités de contrôle et de surveillance de chaque nouvelle procédure d'enquête, unité intégrée ou centre de fusion[12].

Finalement, dans son rapport exhaustif de 2009 portant sur l'enquête du Canada à la suite de l'attentat à la bombe contre un vol d'Air India en 1984, le juge Major a formulé une série de recommandations concernant l'échange de renseignements et les mesures de sécurité aérienne. Il vaut la peine de souligner que le juge Major en est venu à la conclusion que, selon les éléments de preuve et les programmes existants, le système canadien de contrôle des voyageurs est adéquat et solide.

Cette conclusion a grandement soulagé les milieux de la protection de la vie privée et des droits de la personne au Canada qui estimaient depuis un moment que les systèmes de surveillance des passagers et des transports étaient allés trop loin dans le contrôle des

[12] CPVP, *Droits et réalités : augmenter la surveillance des programmes en matière de sécurité nationale du Canada — Mémoire présenté au Comité permanent de la sécurité publique et nationale* (2009), URL : http://www.priv.gc.ca/parl/2009/parl_sub_090507_f.cfm; voir également Andrea Wright, « Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight, and Review », dans *The Human Rights of Anti-Terrorism*, Ottawa, Irwin Law, 2008, p. 327-367.

personnes et avaient négligé de contrôler le *frêt*. Dans son rapport final, concernant le traitement de la sécurité aérienne, le juge Major a d'abord mis l'accent sur le *contrôle du fret* et la *sécurité des installations* qui contiennent la cargaison et les bagages. Nous croyons qu'en mettant l'accent sur le contrôle physique du fret, des biens et des installations, le gouvernement respecte son obligation de limiter la collecte de renseignements personnels et de protéger le droit à la vie privée.

Recommandations du CPVP

1. Mettre en place des mesures de contrôle et des limites claires pour l'échange de renseignements : Bien que le rapport final de l'enquête O'Connor présentait de nombreuses recommandations traitant de problèmes au sein de la GRC, l'importance capitale des contraintes, des mesures de contrôle et des mises en garde concernant l'échange de renseignements demeure. Le Commissariat estime que ces leçons sont toujours aussi importantes aujourd'hui. Nous souhaitons que tous les mécanismes d'échange de renseignements découlant de la Déclaration ou de projets subséquents tiennent réellement compte des recommandations du juge O'Connor et des observations du juge Iacobucci.

2. Étendre la surveillance et remettre en question les fonctions liées à l'analyse transfrontalière des renseignements : L'aspect le plus remarqué du rapport final du juge Iacobucci avait trait au fait que les enquêteurs canadiens du contre-terrorisme n'ont pas su tenir compte de la gravité des conséquences à long terme des étiquettes qu'ils ont apposées à certaines personnes. L'examen et la surveillance de toute nouvelle procédure d'enquête, unité intégrée et centre de fusion constituent une mesure de contrôle critique pour éviter ce genre de problème. La popularité croissante du modèle de fusion occasionne des risques sérieux pour la protection de la vie privée puisque les renseignements personnels provenant d'importantes sources de données intersectorielles (bases de données gouvernementales et commerciales) sont combinés puis redistribués[13]. Le CPVP insiste qu'il faut éviter de mettre en place des ententes dans lesquelles la conservation et le contrôle des renseignements personnels sont incertains ou de faibles mécanismes de responsabilité sont en place pour une utilisation à l'extérieur du Canada.

3. Appliquer le processus d'évaluation des facteurs relatifs à la vie privée (EFVP) : La responsabilité de réaliser une EFVP pour chaque initiative devrait être centralisée au sein du GTPF, idéalement sous l'égide d'une personne détenant une responsabilité claire à l'égard des questions relatives à la vie privée[14]. Ces dispositions devraient être mises en place pour tous les programmes, les composantes ou les ententes subséquentes. Au Canada, le Commissariat devrait être informé de telles initiatives et participer au processus de consultation dès les premières étapes.

---

[13] Torin Monahan, *Surveillance in the Time of Insecurity* (Critical Issues in Crime and Society, 2008); voir également Laura K. Donohue, « Anglo-American Privacy and Surveillance » *Journal of Criminal Law and Criminology, v*ol. 96, n° 3, p. 1059-1208 (mai 2006), URL : http://iis-db.stanford.edu/pubs/21219/Privacy_and_Surveillance.pdf.

[14] Le processus d'EFVP aide à établir si les initiatives comportant l'utilisation de renseignements personnels augmentent les risques pour la protection de la vie privée et permet de mesurer, de décrire et de quantifier ces risques et de proposer des solutions pour éliminer ou réduire ceux-ci à un niveau acceptable. Consulter *Nos attentes : un guide pour la présentation d'évaluation des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada* (2011), URL : http://www.priv.gc.ca/information/pub/gd_exp_201103_f.cfm.

4. Accroître les mesures de protection de la vie privée pour l'échange transfrontalier de données : Comme le soutient le CPVP depuis plusieurs années, les dispositions prévues dans la *Loi sur la protection des renseignements personnels* régissant la communication de renseignements personnels par le gouvernement du Canada à des États étrangers doivent être renforcées :

> *[La* Loi sur la protection des renseignements personnels*] ne prévoit que deux restrictions à la communication de renseignements personnels aux gouvernements étrangers : une entente ou un arrangement doit exister, et les renseignements personnels doivent être utilisés à des fins d'administration ou d'application d'une loi ou d'exécution d'une enquête. La* Loi sur la protection des renseignements personnels *n'exige même pas que l'entente soit écrite. Elle n'impose pas aux institutions qui communiquent des renseignements l'obligation d'établir l'utilisation précise pour laquelle les données seront communiquées, de limiter son utilisation subséquente par le gouvernement étranger à cette fin, de limiter la quantité de renseignements personnels communiqués et de restreindre la communication [...]. [L]a* Loi sur la protection des renseignements personnels *n'impose même pas à l'institution du gouvernement canadien elle-même l'obligation de base de sauvegarder de façon appropriée les renseignements personnels*[15]*.*

Bien que de récentes directives émises par le Secrétariat du Conseil du Trésor aux ministères fédéraux sur les échanges intergouvernementaux offrent un éclairage important sur ces questions, les citoyens s'attendent à ce que des protections aussi fondamentales soient comprises dans une loi, et non seulement dans une politique ou un règlement.

Utilisation de la biométrie : une arme à deux tranchants

Le gouvernement du Canada n'a pas encore adopté de normes législatives concernant les protections minimales pour les données biométriques. En revanche, les organismes internationaux de normalisation ont été actifs au cours de la dernière décennie dans le traitement de la mise en œuvre de la biométrie et ont pris en compte les enjeux liés à la protection de la vie privée, les risques d'identification ou les recours possibles si l'information est utilisée de manière inappropriée. Actuellement, au Canada, l'utilisation d'identifiants biométriques est régie au fédéral par les dispositions de la *Loi sur la protection des renseignements personnels*, qui réglemente la collecte, l'utilisation et la communication des renseignements personnels, ainsi que l'accès à ces renseignements, « quels que soient leur forme et leur support ».

Règle générale, il faut démontrer que toute mesure portant atteinte à la vie privée est nécessaire afin de répondre à un besoin précis. De plus, l'intrusion dans la vie privée doit être proportionnelle à l'avantage qui pourra ainsi être obtenu, et il doit avoir été établi qu'aucune autre mesure moins intrusive n'aurait permis d'atteindre le même objectif[16]. Ensemble, ces

---

[15] CPVP, *Réforme de la* Loi sur la protection des renseignements personnels*,* recommandations (2008), URL : http://www.priv.gc.ca/parl/2008/parl_080429_02_f.cfm#rec10.

[16] Gouvernement du Canada, Direction de la recherche, Division de l'industrie, de l'infrastructure et des ressources, *La biométrie et son usage par l'État* (2010), URL : http://www.parl.gc.ca/Content/LOP/ResearchPublications/06-30-f.htm#ftn16.

trois principes forment les paramètres de base servant à évaluer les nouvelles technologies afin qu'elles aient une incidence minimale sur la vie privée des personnes.

Même quand le traitement des renseignements personnels est jugé approprié en fonction des critères susmentionnés, la manière de le mettre en œuvre est également importante. Un des principes centraux de la protection de la vie privée est de donner aux personnes le contrôle sur la création, la conservation et l'utilisation des renseignements les concernant, ce qui signifie que le moyen par lequel les renseignements biométriques personnels sont stockés est très important pour protéger le droit à la vie privée des Canadiennes et des Canadiens. Les renseignements personnels peuvent être stockés électroniquement dans de vastes répertoires centralisés ou se trouver dans des documents électroniques avec jeton d'authentification conservés par les citoyens. Dans certains cas, il peut sembler que des renseignements personnels sont conservés par des citoyens alors qu'en fait, les renseignements sont stockés de manière centralisée.

La vie privée qui a trait à la personne peut le plus fortement prétendre à une protection constitutionnelle parce qu'elle protège l'intégrité corporelle et plus particulièrement le droit de refuser toute palpation ou exploration corporelle qui dévoilerait des objets ou des matières qu'une personne veut dissimuler. ~ *R. c. Tessling [2004] 3 R.C.S 21*

Le permis de conduire Plus (PC Plus) émis par la Colombie-Britannique, le Manitoba, l'Ontario et le Québec, par exemple, emmagasine des renseignements dans une base de données centralisée et le document permettant l'IRF est simplement un « identifiant » unique qui permet à l'agent des services frontaliers d'accéder rapidement aux renseignements pertinents. De même, les renseignements biométriques peuvent être stockés de manière centralisée dans de vastes bases de données ou dans des documents électroniques avec jeton d'authentification détenus par des citoyens. Le stockage local des données biométriques présente un certain nombre d'avantages relativement à la protection de la vie privée, dont la réduction des risques de collecte secrète d'information, d'utilisation non divulguée à des fins secondaires, d'interliaisons entre des applications ou des programmes, de détournement d'usage et d'atteinte à la protection des données institutionnelles.

Recommandations du CPVP

1. Éviter la centralisation non essentielle des données biométriques : Le CPVP recommande fortement que la mise en place de tout programme de biométrie à la suite de la Déclaration soit assujettie à une structure de gouvernance solide et évite le recours à des bases de données centralisées afin de minimiser le risque d'utilisation secondaire non essentielle des renseignements. Toute forme de registre central pour des renseignements d'une nature aussi délicate doit être assujettie à des mesures de contrôle mis en place dans le cadre d'un mandat précis en vertu d'une loi, et à des mesures de protection de la vie privée comme la limitation de la collecte, la classification, le contrôle de l'accès et la dépersonnalisation.

2. Faire confiance, mais vérifier : L'identification n'exige pas que l'agent de vérification accède à des documents autres que ceux qui concernent la personne, ce qui a pour effet de limiter la visibilité des données privées et d'accroître le respect de la vie privée des personnes. Un système de « comparaison des échantillons » augmente de beaucoup la possibilité d'obtenir de faux positifs, ce qui réduit l'efficacité du système et le respect de la vie privée. L'identification requiert un bon nombre de renseignements biométriques afin de s'assurer d'un bon couplage des données et accroît la tentation de sacrifier la vie privée en faveur de la fiabilité. Pour ces raisons, le CPVP préfère nettement la méthode de la *vérification* à celle de *l'identification*[17].

3. Tenir compte des effets à long terme sur les réseaux des systèmes de contrôle fondés sur la biométrie : Le CPVP invite à la prudence relativement à la mise en œuvre de tout programme de collecte de données biométriques. Quand l'identité est facilement vérifiable à l'aide de la biométrie et qu'elle est combinée à des bases de données réseautées, la possibilité de suivis, voire d'émergence d'une « société de surveillance », est accrue. La collecte à grande échelle d'identifiants biométriques liés à de nombreuses bases de données constitue une atteinte indue à la protection des renseignements personnels privée sans preuve d'efficacité ou d'équité à l'appui[18].

4. Établir des mesures de protection techniques : Des normes élevées doivent également être mises en place pour l'intégrité et la sécurité des renseignements biométriques et des autres renseignements d'identification.

Mise en place d'un système continental d'entrée et de sortie

Étant donné que les économies canadienne et américaine sont de plus en plus liées, tout nouveau processus de sécurité devrait chercher à réduire au minimum les perturbations pour les biens et les personnes qui traversent la frontière. Un modèle de sécurité continental propose la mise en place d'une quelconque « base de données des entrées et sorties » afin de consigner le passage de chaque personne qui transite vers le Canada ou les États-Unis. En plus de la saisie des documents présentés par la personne (passeport, visa, etc.), les adeptes de ce modèle suggèrent l'utilisation d'un identifiant biométrique (empreinte digitale, balayage de la rétine ou de l'iris, etc.) afin de permettre une documentation simple et efficace et de lutter contre la fraude.

Un programme d'une telle envergure constituerait un changement majeur dans la dynamique de notre régime d'échange de renseignements actuel et soulèverait par ailleurs des inquiétudes sérieuses sur le plan de la protection de la vie privée qui vont généralement de pair avec l'utilisation de tout système d'identification biométrique. Le Canada et les États-Unis collaborent déjà dans le contexte des mesures de contrôle des voyageurs (IPV/DP), des contrôles de l'immigration et des processus de contrôle des réfugiés. Toutefois, les répercussions globales sur toutes les personnes touchées par le nouveau modèle — qu'il

---

[17] CPVP, *Des données au bout des doigts. La biométrie et les défis qu'elle pose à la protection de la vie privée* (2011), URL : http://www.priv.gc.ca/information/pub/gd_bio_201102_f.pdf, p.10.

[18] Jay Stanley et Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union, New York, janvier 2003, URL : http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

s'agisse de voyageurs, d'immigrants ou de réfugiés — devraient être examinées afin d'en comprendre les conséquences directes sur le droit à la vie privée tel qu'il est défini dans la Déclaration universelle des droits de l'homme.

Il y a deux principaux modèles de régime d'entrée et de sortie. Le premier est le modèle européen dans lequel les citoyens des États membres obtiennent la liberté de mouvement à l'intérieur des 25 États de l'Union européenne (UE). Les passeports sont soumis au balayage numérique au point d'entrée et les renseignements sont enregistrés et consignés dans le Système d'information Schengen (SIS)[19]. Étant donné que de plus en plus de pays optent pour des documents de voyage lisibles par machine ou équipés d'une puce, les renseignements sont collectés automatiquement, échangés et validés par les administrations douanières de l'UE. Si cet échange de renseignements suscite un intérêt particulier pour un des États membres, le SIS émet alors une alerte de haut niveau à certaines fins très précises : retrouver les personnes disparues, trouver les bagages volés ou résoudre des crimes antérieurs commis à l'intérieur de la région Schengen. Quand le détenteur du passeport quitte l'Union européenne, son point de départ est consigné et transmis à tous les États.

En théorie, quand une personne est admise dans un pays de l'UE, elle obtient le droit de passage dans tous les autres pays sans devoir se présenter à un autre point de contrôle des douanes. La viabilité à long terme de conserver ce modèle d'échange de renseignements intégré reste à voir, et certains des États membres (comme le Danemark, l'Italie et la France) ont commencé à remettre en question son efficacité[20]. Toutefois, les principales inquiétudes relatives à la protection de la vie privée résident dans le fait que les données recueillies du passeport sont échangées avec d'autres pays dans lesquels le détenteur ne passera peut-être même pas.

La deuxième approche est le modèle américain, élaboré principalement à la suite des attentats du 11 septembre 2001. À la fin de 2002, le département de la Sécurité intérieure, récemment formé, mettait en place le National Security Entry – Exit Registration System (NSEERS)[21]. Tout homme âgé de plus 16 ans qui est citoyen d'un pays à « haut risque » (selon le département d'État) était tenu de s'enregistrer à un point d'entrée ou à un bureau du département de la Sécurité intérieure et de fournir des empreintes digitales et des photos. Même s'ils étaient admis légalement dans le cadre du processus de demande de visa, ces étrangers étaient contraints de se rapporter au département de la Sécurité intérieure et de fournir des plans et des mises à jour détaillés de leurs activités pendant leur séjour au pays. Un tel régime démontre comment la réaction immédiate au terrorisme a éclipsé toute inquiétude sous-jacente pour la protection de la vie privée.

À l'opposé du modèle européen qui recueille seulement les photos et offre un accès limité aux organismes nationaux chargés de l'application de la loi, le modèle suivant à voir le jour était le US VISIT[22]. Ce système d'entrées et de sorties est relié au système plus vaste du US

---

[19] Commission européenne, *Schengen Convention Frequently Asked Questions* (2011), URL : http://ec.europa.eu/home-affairs/policies/borders/borders_faq_en.htm.
[20] « Defenders of the Schengen zone face a battle » *Financial Times,* (24 mai 2011), URL : http://www.ft.com/cms/s/0/5f8bfade-8628-11e0-9e2c-00144feabdc0.html#axzz1O7aj8dxk.
[21] Département de la Sécurité intérieure, *Changes to the National Security Entry/Exit Registration System (NSEERS),* (2003), URL : http://www.dhs.gov/xnews/releases/press_release_0305.shtm.
[22] Le United States Visitor and Immigrant Status Indicator Technology (US-Visit) est considéré comme la version élargie du programme NSEERS d'origine.

Interagency Border Inspection System (IBIS). Même l'évaluation du risque commence à converger entre ces systèmes segmentés. Être identifié comme une menace dans l'IBIS, par exemple, peut donner lieu à l'ajout de personnes sur la liste des personnes interdites de vols aux États-Unis. De plus, l'IBIS est lié au National Crime Information Center (NCIC) du FBI, à la police d'État, au National Law Enforcement Telecommunications System (NLETS), ainsi qu'à 20 autres organismes dont Interpol, le Internal Revenue Service et les services secrets[23].

En comparaison, l'Agence des services frontaliers du Canada conserve un registre de tous les déplacements des Canadiens qui entrent et sortent du pays par voie aérienne pendant sept ans au moyen de la carte de déclaration douanière (E-311). Toutefois, cette base de données peut *seulement* être utilisée à des fins très précises énumérées dans l'entente et elle n'est pas entièrement intégrée avec les bases de données nationales d'application de la loi des États membres. Inutile de dire que la manière dont des renseignements personnels d'une nature aussi délicate sont échangés avec les autres gouvernements doit être une des considérations premières des responsables canadiens lors de l'examen des diverses possibilités pour tout protocole de suivi des passagers à grande échelle.

Au moment d'entrer aux États-Unis en tant que personnes privées, de nombreux visiteurs étrangers fournissent maintenant des renseignements personnels (notamment des photos et des empreintes digitales) que leur propre gouvernement pourrait uniquement exiger d'eux s'ils étaient détenus pour crime. En adaptant le modèle de l'UE pour répondre à nos propres besoins en matière de sécurité, le gouvernement du Canada pourrait être mieux à même de protéger les frontières et d'assurer un commerce efficace avec les États-Unis. Bénéficiant de l'expérience de l'UE, cette adaptation pourrait se faire d'une manière qui reconnaît et qui donne tout le poids souhaité à l'importance que les Canadiennes et Canadiens continuent d'accorder au droit à la vie privée tout en limitant le risque que les renseignements personnels soient utilisés à des fins secondaires sans lien avec la sécurité.

Recommandations du CPVP

1. Tenir compte sérieusement du schéma de protection des données européen de même que de l'expérience accumulée : Le gouvernement devrait défendre l'adoption d'un modèle typiquement canadien largement influencé par l'approche européenne, c'est-à-dire un modèle qui reflète les préoccupations des Canadiennes et Canadiens pour la protection de leurs renseignements personnels. En recueillant seulement les renseignements qui sont véritablement nécessaires pour la sécurité frontalière, un tel programme devrait limiter le danger de collecte de renseignements superflus et leur utilisation inappropriée. En comparaison, l'adoption d'un modèle américain signifierait pour le Canada l'échange de renseignements personnels sur les voyageurs s'adonnant à des visites locales et dans certains cas, sur des personnes ayant pris consciencieusement la décision de ne pas se rendre aux États-Unis. Une telle approche serait non seulement une atteinte aux valeurs traditionnelles des Canadiennes et des Canadiens à l'égard de la vie privée, mais elle pourrait également avoir pour conséquence de nuire à la réputation du Canada à l'étranger

[23] United States Customs and Border Protection, *IBIS- Who Uses Interagency Border Inspection System* (2010), URL : https://help.cbp.gov/app/answers/detail/a_id/152/~/ibis---who-uses-interagency-border-inspection-system.

en tant que destination de choix. Les considérations suivantes doivent être étudiées attentivement dans le choix d'un modèle pour la sécurité à l'intérieur du périmètre :

- *L'usage premier de ces données est-il lié à la sécurité à la frontière ou à l'application de la loi?*
- *Quel type de données biométriques sera requis pour ce nouveau programme?*
- *Qui supervise l'utilisation adéquate de ces données?*
- *Quelles bases de données seront liées à ce programme?*
- *Où et comment les données seront-elles stockées?*
- *Quels recours seront accordés par le gouvernement du Canada en cas d'accès secondaire illégal?*
- *Comment les personnes possédant une double nationalité seront-elles classées?*
- *Comment les différends au sujet des pays « étiquetés », en particulier Cuba, seront-ils traités?*

2. Les deux gouvernements devraient expliquer clairement aux citoyens les objectifs du programme : Règle générale, les systèmes de contrôle des entrées et des sorties sont en premier lieu des systèmes de gestion des frontières. Ils offrent une manière de contrôler l'immigration et la sécurité, et de percevoir les droits. Les citoyens et les visiteurs des États-Unis et du Canada doivent être parfaitement informés des objectifs des programmes, de l'étendue de leur application, de l'utilisation des renseignements personnels ainsi que de la manière dont les renseignements personnels seront adéquatement protégés.

3. Tenir compte des répercussions associées à une augmentation de la collecte de renseignements personnels : En général, l'utilisation de données biométriques, comme les empreintes digitales, à des fins secondaires soulève des inquiétudes non seulement en ce qui a trait à la protection de la vie privée, mais aussi pour la protection d'autres droits de la personne (comme la mobilité). Par exemple, si un réfugié est incapable de transmigrer et « d'atterrir » où que ce soit, la fuite en cas de contrainte et de danger devient pratiquement impossible. Même à l'échelle nationale, la mise en place d'un système national de sortie est controversée. Il y a eu beaucoup de contestation aux États-Unis concernant le coût d'une infrastructure de collecte des empreintes digitales à tous les points de départ. Outre la protection de la vie privée, le coût, les répercussions non intentionnelles et les autres complications possibles doivent être pris en compte.

Cybersécurité, renseignements personnels et surveillance électronique

Les deux pays reconnaissent que le domaine du numérique est devenu partie intégrante de l'infrastructure critique, et des mesures ont été prises pour assurer sa défense. Les communications privées et sécurisées sont effectivement une composante essentielle de nos économies et de nos sociétés élargies. Le CPVP appuie généralement ces mesures, pourvu qu'elles tiennent bien compte des préoccupations de nos citoyens pour la protection de la vie privée, que ce soit en ligne ou non.

La question de la cybersécurité a une grande importance puisque tant les entreprises que les ministères doivent s'assurer que les renseignements personnels recueillis auprès des

citoyens ne sont pas accessibles aux entités non autorisées. Aux États-Unis, la stratégie internationale pour le cyberespace, publiée récemment, reconnaît et réitère l'engagement premier du gouvernement envers la protection juridique des citoyens, en plus de soutenir fermement que les libertés fondamentales, la protection de la vie privée et la libre circulation de l'information sont des idéaux qui ne peuvent être compromis, que ce soit en ligne ou non[24].

De même, comme l'énonce la Stratégie de cybersécurité du Canada, nos efforts pour corriger ces problèmes doivent être conformes aux valeurs canadiennes comme la primauté du droit, la responsabilité et la protection de la vie privée[25]. Au cours de la dernière décennie, le Canada a entrepris certaines actions visant l'amélioration de sa propre cybersécurité. Des efforts ont également été déployés à l'échelle du gouvernement pour mieux protéger les citoyens et les entreprises des risques et des menaces du Web.

Les programmes de cybersécurité doivent reconnaître les questions relatives à la souveraineté et à l'intégrité soulevées par la conservation de données locales sur les serveurs et systèmes canadiens. Ceux-ci contiennent des renseignements personnels qui ne doivent être ni compromis ni menacés. Les intérêts en ligne associés aux enquêtes de sécurité nationale et d'application de la loi, dans une tentative de contrôle des systèmes en ligne et des réseaux, ne peuvent aller de l'avant sans une procédure établie, une surveillance adéquate et un examen attentif. Les gouvernements canadien et américain ont compris que la protection de la vie privée et la sécurité ne sont pas incompatibles[26].

Le droit de l'État de déceler et de prévenir le crime commence à l'emporter sur le droit du particulier de ne pas être importuné lorsque les soupçons font place à la probabilité fondée sur la crédibilité. L'histoire confirme la justesse de cette exigence comme point à partir duquel les attentes en matière de la vie privée doivent céder le pas à la nécessité d'appliquer la loi.

~ Hunter et autres c. Southam inc. [1984] 2 R.C.S. 145

Le CPVP a appuyé les efforts déployés à ce jour par le Canada pour la cybersécurité, en particulier ceux visant à combattre efficacement le pollupostage et le vol d'identité. Voilà deux exemples de cybermenaces visant à exploiter les renseignements personnels de citoyens peu méfiants à des fins de fraude, de fabrication de faux documents ou d'autres activités criminelles. Bien entendu, nous continuons à alléguer que du travail reste à faire pour régler ces problèmes, en particulier parce qu'ils surviennent en ligne et que, bien souvent, les victimes ne se doutent pas du tout qu'elles ont été ciblées.

Toutefois, les principes juridiques fondamentaux et les mesures de protection de la vie privée traditionnelles qui s'appliquent dans le monde réel doivent dans tous les cas s'appliquer au cyberespace. La *Loi sur la protection des renseignements personnels et les documents*

---

[24] La Maison-Blanche, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (mai 2011), p. 5, URL : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[25] Sécurité publique Canada, *Stratégie de cybersécurité du Canada. Renforcer le Canada et accroître sa prospérité* (2010), p. 8, URL : http://www.securitepublique.gc.ca/prg/ns/cbr/_fl/ccss-scc-fra.pdf.
[26] Mary Ellen Callahan, « The Privacy Framework for Information Sharing in Security and Border Management: A U.S Perspective » *One Issue, Two Voices,* vol. 13, Woodrow Wilson International Center for Scholars (2010), URL : www.dhs.gov/.../privacy/dhsprivacy-privacyandinformationsharing-issue13-october2010.pdf.

électroniques (LPRPDE) du Canada, applicable au secteur privé, a été édictée pour garantir aux Canadiennes et aux Canadiens que leur droit à la vie privée, en tant que citoyens et consommateurs, s'applique également au domaine numérique lorsqu'ils sont en ligne pour discuter, faire des achats ou naviguer sur Internet. L'assurance que le commerce et les communications électroniques ont cours dans un espace digne de confiance doit être un des engagements clés du gouvernement au moment où le Canada tente de se joindre aux efforts actuels des États-Unis en matière de cybersécurité.

Recommandations du CPVP

1. Renforcer la protection fondamentale et le respect des droits et libertés en ligne : La collaboration et la collecte de renseignements par le gouvernement dans un contexte de cybersécurité ne devraient pas prendre de l'ampleur au détriment de la protection de la vie privée des personnes, des libertés civiles et des garanties constitutionnelles. Les décideurs et les enquêteurs doivent garder à l'esprit que les citoyens attendent d'eux qu'ils maintiennent cet équilibre essentiel. Il serait ironique, voire nuisible, que dans notre empressement à sécuriser nos systèmes électroniques pour les communications et le commerce, par l'entremise d'une sécurité et d'une surveillance accrues, nous en venions à miner la confiance que les citoyens ont envers la confidentialité et le caractère privé de leurs propres communications. Le Canada et les États-Unis devraient entamer des pourparlers sur la collaboration en matière de cybersécurité en ayant conscience de ce risque et sachant précisément quelles initiatives sont inacceptables.

2. Éviter les solutions et les stratégies purement techniques : Pour ce faire, les deux gouvernements doivent élargir leur approche à l'égard du cyberespace. La sécurité ne peut se limiter simplement à une augmentation des dépenses pour des solutions techniques. Les menaces omniprésentes comme l'hameçonnage, le pollupostage, les réseaux de zombies, les maliciels et les espiogiciels ne peuvent être contrées dans les sphères publiques et privées sans une stratégie à grande échelle[27]. Tout effort commun doit comprendre des directives juridiques claires, définissant ce qui est et n'est pas acceptable. Il doit également s'accompagner d'une éducation et d'une sensibilisation du public à la sécurité des données et aux pratiques de protection des renseignements personnels à grande échelle, d'efforts renforcés pour soutenir la recherche indépendante et multidisciplinaire sur les enjeux du cyberespace, d'un engagement binational pour la mise en œuvre de normes de sécurité offrant une meilleure protection de la vie privée et de l'assurance que les organismes de réglementation ont la capacité et l'autorité requises pour garantir de meilleures pratiques au sein de l'industrie.

3. Élargir la consultation publique, le dialogue, la sensibilisation et l'engagement : Le manque d'engagement du public, de rapports publics ouverts et de transparence dans les efforts pour améliorer la cybersécurité est source de confusion et de critiques continues au Canada et aux États-Unis. La rareté des sources ouvertes d'information et de discussions laisse le citoyen moyen (de même que de nombreux spécialistes) complètement à l'écart des politiques et des discussions juridiques portant sur la sécurité en ligne. À l'ère du numérique,

[27] Ron Deibert, Centre canadien des études sur la sécurité mondiale à l'École Munk des affaires internationales de l'Université de Toronto, « Cyber Security: Canada Is Failing The World » (26 mai 2011), URL : http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html.

où les citoyens veulent de l'engagement et de l'interaction, cette absence de dialogue ouvert est clairement inacceptable et nuira aux efforts à long terme. Les responsables canadiens et américains doivent créer des mécanismes pour communiquer régulièrement des rapports publics, permettre l'engagement et mettre en place un processus ouvert pour écouter les préoccupations et les plaintes au moment où débutent les efforts de collaboration en matière de cybersécurité. Ces tribunes ne doivent pas voir le jour en fin de parcours; elles doivent être planifiées, substantielles et interactives dès le début.

4. Élargir la recherche publique et le dialogue au sujet des défis internationaux liés à la cybersécurité : La cybersécurité est devenue une préoccupation majeure des gouvernements du monde entier et, pourtant, une trop grande partie de l'expertise, de la recherche et des discussions demeure cachée du public. Une participation beaucoup plus importante du milieu universitaire, de la société civile, des médias et des citoyens est nécessaire. J'encouragerais les gouvernements du Canada et des États-Unis à explorer des solutions créatives pour encourager une recherche publique stable et à long terme dans ce domaine. Au Canada, nous avons plusieurs centres d'excellence en émergence dans ce domaine, mais le sujet à l'étude est vaste et profond. Il faudrait inciter les universités du Canada et des États-Unis à développer leur intérêt et leur expertise sur le sujet, à mettre en place des réseaux et à organiser des événements conjoints pour partager leurs recherches. L'approvisionnement libre, les discussions transparentes et le débat ouvert sur la cybersécurité et sur les questions de protection de l'infrastructure devraient être la norme, pas l'exception. Personne ne détient le monopole des bonnes idées (ou des mauvaises expériences) dans ce domaine, et les leçons retenues dans un secteur, un contexte ou un pays en particulier peuvent présenter une valeur inestimable pour le grand public. Il faudra de l'argent, du temps et des personnes (pas des systèmes), mais comme c'est le cas pour la formation et l'investissement dans le capital humain, le gain à venir sera extraordinaire.

Protection de la vie privée dans les interventions sanitaires d'urgence

Les inquiétudes du public relativement à l'éclosion de pandémies s'accroissent à mesure que les frontières deviennent plus perméables aux biens et aux personnes. La grande préoccupation à l'égard de la maladie de la vache folle en 2001, de l'épidémie de SRAS en 2003 et du virus H1N1 en 2009 montre bien la capacité qu'ont les menaces biologiques de se répandre rapidement partout dans le monde. Les gouvernements et les organisations supranationales, comme l'Organisation mondiale de la santé (OMS), ont commencé à reconnaître que la seule manière de prévenir les éclosions régionales de maladies contagieuses est d'identifier rapidement les zones problématiques afin de les mettre en quarantaine et d'empêcher ainsi que l'épidémie se propage dans le monde et se transforme en pandémie.

Bien que les mesures d'hygiène et les soins médicaux appropriés soient évidemment les premiers moyens de défense contre les maladies, l'OMS a découvert que les programmes internationaux d'échange de renseignements sont nécessaires afin de suivre la piste de la

dissémination et de tenter de la localiser[28]. Aussi importante qu'elle puisse être, la divulgation de ces données constitue une atteinte à la protection des renseignements personnels du patient de la part des hôpitaux et des autorités sanitaires. Les Canadiennes et les Canadiens ont des attentes élevées en matière de vie privée en ce qui a trait aux documents et aux antécédents médicaux. Les installations médicales se montrent le plus souvent prudentes relativement à la divulgation, mais il n'y a actuellement aucune procédure législative en place, mis à part dans un « état d'urgence », qui stipule comment les alertes et la planification devraient s'effectuer. Les atteintes à la protection des renseignements personnels doivent donc être évaluées en fonction du potentiel de l'épidémie de se transformer en pandémie. En l'absence de mesures de protection législatives adéquates, les données sont souvent divulguées à la suite de simples décisions discrétionnaires.

Cette situation est très problématique puisque les dossiers médicaux sont généralement considérés comme étant encore plus importants que les identifiants biométriques. Ils contiennent des renseignements personnels qui ont été perçus comme inviolables à travers l'histoire et qui sont assujettis à la plus stricte confidentialité éthique et professionnelle. La Cour suprême du Canada a également reconnu que les dossiers médicaux doivent être conservés selon les normes les plus strictes. Comme le juge LaForest l'a indiqué, « l'utilisation du corps d'une personne, sans son consentement, en vue d'obtenir des renseignements à son sujet, constitue une atteinte à une sphère de la vie privée essentielle au maintien de sa dignité humaine[29]. » Les données relatives aux dossiers médicaux doivent être protégées avec le plus grand soin parce que « la confiance que le public doit avoir dans l'administration des services médicaux serait mise à rude épreuve si l'on devait autoriser la circulation libre et informelle de renseignements [...] des hôpitaux vers la police[30]. »

Le risque de détournement d'usage est amplifié lorsque les données en question proviennent de dossiers médicaux. La communication des dossiers médicaux des hôpitaux aux représentants de la loi est perçue, tant dans le domaine légal que civil, comme une atteinte importante à la vie privée d'une personne. La divulgation de ces documents à des entités étrangères est contestée puisque le contrôle du flux des données ne peut être réglementé. Comme dans le cas des identifiants biométriques, il y a de nombreux cas où les dossiers médicaux pourraient être utilisés à des fins secondaires. Il est évident que si un tel régime n'est pas créé avec le plus grand soin pour la vie privée, le risque que le public ait des inquiétudes est très élevé.

L'utilisation du corps d'une personne, sans son consentement, en vue d'obtenir des renseignements à son sujet, constitue une atteinte à une sphère de la vie privée essentielle au maintien de sa dignité humaine. […]La confiance que le public doit avoir dans l'administration des services médicaux serait mise à rude épreuve si l'on devait autoriser la circulation libre et informelle de renseignements [...] des hôpitaux vers la police.
~ R. c. Dyment, [1988] 2 R.C.S. 417

[28] Organisation mondiale de la santé, *Pandemic Influenza Preparedness Framework for the Sharing of Influenza Viruses and Access to Vaccines and Other Benefits* (2011), URL : http://www.who.int/csr/disease/influenza/pip_framework_16_april_2011.pdf.
[29] *R. c. Dyment,* [1988] 2 R.C.S. 417, paragr. 27.
[30] *R. c. Dyment,* [1988] 2 R.C.S. 417, paragr. 38.

Recommandations du CPVP

1. **Adopter des cadres législatifs appropriés :** Ces cadres doivent régir l'échange de renseignements dans les partenariats pour la sécurité de la santé mentionnés dans la Déclaration. Ils devraient viser à garantir un équilibre adéquat entre le droit à la vie privée et les pouvoirs de réglementation ainsi que la transparence, le signalement et la responsabilité des entités assujetties à la loi et à l'égard du public.

2. **Cerner à l'aide de définitions précises les situations permettant l'échange des renseignements médicaux des Canadiennes et des Canadiens :** Nous suggérons d'appliquer le critère des motifs raisonnables pour étayer la décision de divulguer des renseignements et de limiter les renseignements personnels communiqués à ceux qui sont directement pertinents pour l'urgence sanitaire précisée. Nous proposons aussi que l'entente sur l'échange de renseignements prévoie que les renseignements divulgués soient dépersonnalisés ou anonymisés si cela permet d'atteindre l'objectif fixé.

3. **La divulgation des renseignements doit être aussi limitée et précise que possible :** Les renseignements personnels ne devraient pas être utilisés par le destinataire à des fins autres que celles pour lesquelles ils ont été communiqués. Ils devraient être protégés à l'aide de mesures de sécurité adéquates et devraient uniquement être conservés pour la période nécessaire à l'atteinte des objectifs liés à l'urgence sanitaire en question. De plus, le destinataire devrait avoir l'obligation d'assurer la confidentialité des renseignements à moins qu'une obligation d'origine législative le force à les divulguer.

Conclusion

Les lois canadiennes et américaines diffèrent sur certains points essentiels, notamment : ce qui constitue une attente raisonnable en matière de vie privée, ce qui constitue un renseignement personnel, et les conséquences juridiques d'un transfert de renseignements à une tierce partie. Toutefois, en dépit de ces différences, le CPVP ne croit pas que les Canadiennes et les Canadiens soient prêts à accepter un « nivellement par le bas » des mesures de protection de la vie privée pour l'adoption d'un programme élargi de sécurité du périmètre.

Le CPVP croit qu'aucune entente subséquente d'échange de renseignements ne devrait être conclue jusqu'à ce qu'un cadre législatif amélioré ait été mis en place afin de permettre une surveillance et des mesures de protection de la privée adéquates et qu'il y ait eu une discussion et un débat publics concertés dans nos assemblées respectives.

Compte tenu de la nécessité fondamentale de protéger les libertés civiles et la vie privée dans le cadre de l'élaboration d'une stratégie de sécurité du périmètre nord-américain, et du fait que certaines mesures portant atteinte à la vie privée ne soient pas efficaces, nous incitons les deux gouvernements à tenir dûment compte de nos recommandations et à les intégrer en tant qu'aspects fondamentaux de leur vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre.

ANNEXE — Lettre de la commissaire à la protection de la vie privée du Canada à M. Simon Kennedy du Groupe de travail par-delà la frontière pour donner suite à la signature de la déclaration *Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre*

Monsieur Simon Kennedy
Sous-ministre délégué principal
Industrie Canada
235, rue Queen, 11e étage
Tour Est, bureau 1114A
Ottawa (Ontario) K1A 0H5

Monsieur,

Je vous écris pour donner suite à notre rencontre du mois dernier et vous remercier de la réunion d'information sur la Déclaration par-delà la frontière et sur le travail de votre groupe qui en a découlé. Nous comprenons que les renseignements fournis en sont, pour le moment, à l'étape de la conception et qu'il reste beaucoup de place à la négociation. Le Commissariat a l'intention de fournir au Groupe de travail par-delà la frontière des commentaires plus détaillés lorsque votre consultation publique commencera en mai. Toutefois, étant donné l'évolution rapide des travaux et le fait que les principes conjoints de protection de la vie privée sont déjà en cours d'élaboration, nous souhaitions vous faire part de quelques réflexions préliminaires sur cette importante première étape.

Contexte international

Évidemment, nous comprenons l'importance de faciliter le commerce et d'assurer la sécurité à la frontière. Toute révision de mesures ou toute nouvelle initiative pour éliminer certains obstacles ou retards que vivent actuellement de nombreux voyageurs seraient les bienvenues. Par ailleurs, la Déclaration vise également l'expansion d'un autre projet, à savoir l'adoption d'une approche intégrée de l'évaluation des menaces dans un objectif de sécurité collective. Comme vous le savez, les mesures de sécurité mondiales prises au cours de la dernière décennie ont eu des répercussions à la fois sur le droit à la vie privée et sur la liberté de mouvement. Bien que la sécurité des voyageurs et des collectivités soit importante, tant pour le Canada que pour les États-Unis, nos approches diffèrent souvent.

À titre d'exemple, si l'évaluation du risque que représente le voyageur ou l'application transfrontalière des lois doivent commencer par un échange accru de renseignements, il est extrêmement important que cet échange soit effectué en accord avec nos valeurs nationales et nos traditions juridiques, comme l'indiquent la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. Il est également primordial que l'échange de renseignements soit :

- limité aux éléments précis des renseignements personnels qui sont réellement nécessaires;
- lié à une utilisation et une communication à des fins très précises;
- soumis à des mesures de protection robustes et à de la surveillance.

Lignes directrices de l'OCDE

Comme vous l'avez mentionné lors de notre rencontre, les *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* datant de 1980 peuvent servir de point de départ à cette réflexion. Je comprends que cet aspect du travail est mené par des représentants du ministère de la Justice et de Sécurité publique Canada. Bien que le rôle que peut jouer le Commissariat soit manifestement limité par son statut d'organisme indépendant du Parlement, nous serions heureux de partager notre expérience des enjeux transfrontaliers relatifs aux données et des instruments internationaux gouvernant la protection des données et le droit à la vie privée.

Il faut toutefois mentionner que les Lignes directrices sont elles-mêmes à l'étude. Après trente ans, sous la direction du Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée, de nombreux membres commencent à réexaminer et à remettre en question la relation entre les Lignes directrices et le nouveau contexte mondial. De nombreuses administrations envisagent des améliorations importantes à la protection de la vie privée, par exemple à la Directive sur la protection des données adoptée par l'Union européenne. Il va sans dire que notre entente actuelle avec de nombreux pays concernant les mesures de protection de la vie privée que nous défendons pourrait être influencée par les changements entrepris avec les États-Unis. Il faut donc garder à l'esprit cette évolution continue de la règlementation entourant les données personnelles.

Expérience canadienne de gouvernance en matière de protection des renseignements personnels

Enfin, j'aimerais également saisir cette occasion pour souligner brièvement quelques points et leçons tirés de l'examen des initiatives transfrontalières entrepris par le Commissariat. En général, je constate que les Canadiennes et les Canadiens ont de grandes attentes en matière de vie privée et qu'ils adhèrent largement au principe de protection des renseignements personnels. Compte tenu des points sensibles en matière de renseignements personnels et de souveraineté, je tends à croire que toute tentative de s'éloigner de ces normes éclipserait rapidement le débat public sur les plans d'action.

Il sera donc extrêmement important de respecter les normes canadiennes de protection des renseignements personnels. Comme nous l'avons maintes fois observé dans nos recherches et dans nos vérifications, l'échange transfrontalier de données doit être entrepris de manière transparente et assujetti à des mesures de contrôles spécifiques. Toute circulation transfrontalière de données devrait faire l'objet de comptes rendus détaillés afin de mieux en informer le Parlement et la population canadienne.

Comme nous en avons discuté, le Commissariat est heureux de pouvoir rappeler les principes généraux de protection de la vie privée qui pourront aider à l'élaboration de cette initiative. La transparence, dans le traitement de ces questions, est essentielle à la confiance et au meilleur intérêt du public. Une solide protection de la vie privée et reddition de comptes sont essentielles pour traiter des préoccupations du public relativement à la circulation des renseignements personnels entre le Canada et les autres pays. À cette fin, je profite de l'occasion pour réitérer ce qui suit :

1. Les renseignements personnels des citoyens devraient être recueillis, utilisés, conservés ou communiqués uniquement s'ils ont un lien direct avec un programme ou une activité spécifique.

2. Les renseignements personnels des citoyens devraient être exacts, à jour, complets et conservés uniquement pour la période de temps prescrite ou nécessaire.

3. Les renseignements personnels des citoyens devraient être protégés physiquement et électroniquement des atteintes ou accès non autorisés.

4. La responsabilité devrait être clairement définie et maintenue.

5. Des mesures de sécurité devraient être mises en place pour veiller à ce que l'accès à un service sélectionné soit séparé de l'accès aux autres services et que les données concernant ces accès ne soient pas partagées avec les autres services.

6. Toute externalisation ou tout rôle élargi attribué aux entreprises du secteur privé pour exécuter des fonctions et activités actuelles du gouvernement, ou de la surveillance devraient se baser sur le *Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché* du Conseil du Trésor du Canada, en particulier pour ce qui est des exigences sur le plan de la sécurité, de l'accès des employés, des inspections, des vérifications et des avis d'incident.

7. Toute entente d'échange d'information devrait respecter le *Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels*.

8. Finalement, dans le cadre de toute nouvelle initiative législative, règlementation en matière de sécurité ou proposition de programme de surveillance, le gouvernement doit évaluer les possibles effets d'entraînement sur notre conception d'une « société libre et démocratique », ce qui signifie que dans le cas où de nouvelles mesures de sécurité pourraient mener à des intrusions et à des pertes sur le plan de la vie privée, le gouvernement devrait être prêt à démontrer :

    a. que ces nouvelles mesures sont nécessaires pour résoudre un problème donné;
    b. qu'il s'agit d'une réponse raisonnable et proportionnelle à un problème en particulier;
    c. qu'elles seront efficaces pour traiter un problème unique;
    d. que la mesure proposée est la solution la moins invasive possible.

Encore une fois, nous sommes heureux d'avoir eu la chance d'échanger nos idées sur les meilleures manières de renforcer les principes de protection de la vie privée et d'appuyer le travail à venir. À court terme, si vous ou les membres de votre groupe de travail désirez de nouveaux commentaires ou de nouvelles idées, veuillez communiquer avec Chantal Bernier au 613-944-4289.

En vous remerciant de l'attention que vous porterez à ces inquiétudes, veuillez agréer, Monsieur, l'expression de mes sentiments distingués.

La commissaire à la protection de la vie privée du Canada,

Jennifer Stoddart