Office of the Privacy Commissioner of Canada
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 publique au 21e siècle

Document de référence émis par le Commissariat à la protection de la vie privée du Canada

Novembre 2010

Table des matières

Sommaire

Le présent document de référence propose une démarche globale en vue de l'analyse de la protection de la vie privée dans le contexte des objectifs stratégiques généraux en matière de sécurité publique et nationale. Il donne un aperçu des étapes fondamentales et du cadre analytique utilisés par le Commissariat à la protection de la vie privée pour examiner des mesures législatives et des propositions de programmes, ou pour effectuer des examens de conformité par l'entremise des fonctions de vérification et d'enquête. Il fait suite à des discussions tenues avec de hauts fonctionnaires fédéraux, des praticiens, des chercheurs, des universitaires et des représentants de la société civile, et vise à fournir une orientation dans le contexte de l'intégration des mesures de protection de la vie privée dans les nouveaux objectifs de sécurité publique et nationale.

Il faut toutefois clarifier deux concepts juridiques afin de comprendre ce cadre : en premier lieu, ce que signifie « renseignements personnels » et, en deuxième lieu, ce qui constitue une « attente raisonnable en matière de vie privée ». Ces deux définitions clés font l'objet d'une discussion. Les détails relatifs à quatre étapes au cours desquelles il faut prendre en compte la protection de la vie privée — la conception, la création, la mise en œuvre et l'examen — seront par la suite présentés en détail en vue de l'élaboration et de la mise en œuvre des programmes et politiques touchant la sécurité.

L'étape 1 porte sur la justification et les motifs de la collecte des renseignements personnels au moment de la conception d'une politique ou d'un programme. Cette étape nécessite la prise en compte du « critère en quatre parties » utilisé par les tribunaux et les conseillers juridiques afin de déterminer si une loi ou un programme peut légitimement annuler ou suspendre des droits comme celui à la vie privée.
Les quatre parties de ce critère (nécessité, proportionnalité, efficacité et intrusion minimale) sont présentées en langage clair.

Le fondement de la collecte des données étant établi au moment de concevoir le programme, **l'étape 2** vise ensuite la sécurité, l'utilisation (comme le couplage de données), la communication et la conservation appropriées des renseignements recueillis. Cette étape nécessite la prise en compte d'un deuxième ensemble de normes reconnues à l'échelle internationale, soit les principes équitables en matière de renseignements, qui peut orienter les organisations tant commerciales que gouvernementales dans l'élaboration d'un programme pour lequel des renseignements personnels seront utilisés.

L'étape 3 vise à déterminer le besoin de pratiques continues de gouvernance et de protection de la vie privée au fil des opérations du programme. Des exemples concrets de ces politiques et pratiques sont expliqués et accompagnés de références à l'ensemble des politiques et rapports fédéraux établis par le Secrétariat du Conseil du Trésor (SCT) relativement à la protection de la vie privée et des données.

La dernière partie du document aborde les contrôles externes — **l'étape 4** — ainsi qu'une série de suggestions en vue d'un examen et d'une surveillance à plus long terme des organisations afin d'assurer la protection de la vie privée et l'élaboration de saines pratiques de traitement des renseignements personnels dans le cadre des initiatives en matière de sécurité publique.

Introduction

Le présent document vise à présenter les étapes fondamentales et le cadre analytique utilisés par le Commissariat à la protection de la vie privée du Canada (le Commissariat) pour examiner de nouvelles mesures liées à la sécurité publique. La même perspective est adoptée pour examiner les mesures législatives et les propositions de programmes, ou pour effectuer des examens de conformité par l'entremise des fonctions de vérification et d'enquête. Ce document vise à orienter les décideurs, les praticiens, les chercheurs et les citoyens quant à l'intégration des mesures de protection de la vie privée dans les nouveaux objectifs relatifs à la sécurité publique et nationale.

En tant qu'organisme indépendant du Parlement, le Commissariat soumet à la réflexion des parlementaires un point de vue orienté sur la protection de la vie privée au sujet des projets de loi et des propositions de programmes. Le Commissariat examine aussi les pratiques de traitement des renseignements personnels de tous les ministères fédéraux. Étant donné que les enjeux touchant la sécurité publique sont devenus le point de mire du gouvernement du Canada au cours des dernières années, les questions relatives à la protection de la vie privée jouent un rôle de plus en plus important dans le cadre des débats portant sur les lois et les politiques publiques.

Des études et des événements récents — dont un vaste examen gouvernemental des politiques en matière de sécurité, la tenue d'événements internationaux par le Canada comme les Jeux olympiques d'hiver et les sommets du G-8 et du G-20 ainsi que le rapport final de l'enquête Major sur l'attentat à la bombe commis contre le vol 182 d'Air India — continuent d'illustrer les enjeux de protection de la vie privée et de sécurité. En mars 2009, la vérificatrice générale du Canada a choisi d'aborder le renseignement stratégique et le partage de renseignements dans son rapport annuel. Elle affirmait alors que « [l]a population canadienne fera confiance aux organismes de sécurité et de renseignement si elle sait que les ministères et organismes gouvernementaux maintiennent un équilibre entre la protection de la vie privée des citoyens et la sécurité nationale[1] .» Le présent document vise à contribuer à ces efforts.

Étant donné que les enjeux touchant la sécurité publique sont devenus le point de mire du gouvernement du Canada au cours des dernières années, les questions relatives à la protection de la vie privée jouent un rôle de plus en plus important dans le cadre des débats portant sur les lois et les politiques publiques.

Pour intégrer le respect de la vie privée dans les initiatives liées à la sécurité, on doit noter le point de vue de la commissaire à la protection de la vie privée de l'Australie, à savoir que toute diminution des mesures de protection doit être une réaction nécessaire à un problème clairement défini, être proportionnelle au risque présenté et être accompagnée de mécanismes d'examen et de reddition de comptes adéquats[2]. Le Commissariat partage ce point de vue.

[1] Bureau du vérificateur général du Canada, Rapport de mars 2009 de la vérificatrice générale du Canada — Chapitre 1 — La sécurité nationale : l'échange de renseignements et d'information — adresse URL : http://www.oag-bvg.gc.ca/internet/Francais/parl_oag_200903_01_f_32288.html.
[2] Commissariat à la protection de la vie privée de l'Australie, *Submission on the Inquiry into the*

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

En offrant un point de vue d'ensemble — plutôt qu'une réponse réactive aux particularités d'un programme donné —, le présent document présente une perspective et détaille des préoccupations qui devraient être pertinentes pour toute nouvelle initiative en matière de sécurité.

Independent Reviewer of Terrorism Laws Bill (septembre 2008), p.2, adresse URL [en anglais seulement] : http://www.aph.gov.au/senate/committee/legcon_ctte/terrorism/submissions/sub06.pdf.

Préambule : La vie privée et sa valeur sociale pour les Canadiennes et les Canadiens

On convient généralement que le droit à la vie privée est une des conditions préalables au maintien de la liberté et de la démocratie. Ce lien habilitant fait en sorte que la vie privée est un droit de la personne reconnu à l'échelle internationale. Au Canada, il s'agit d'un droit garanti par la *Charte canadienne des droits et libertés* (la *Charte*). Dans de nombreux pays, la défense de ce droit a justifié l'adoption de lois pour protéger la vie privée et les données au cours de la deuxième moitié du siècle dernier.

Depuis l'instauration des principes démocratiques, les sociétés considèrent qu'il est essentiel de limiter la capacité du gouvernement à envahir une propriété privée ou l'espace personnel d'une personne, à porter atteinte à sa réputation ou à faire un usage indu de ses renseignements personnels. Une intrusion injustifiée dans la vie personnelle des citoyens est aux antipodes d'un État solide et confiant. Un système rigoureux de freins et de contrepoids a justement été créé pour garantir que les citoyens bénéficient d'un grand espace social leur permettant de profiter de leur vie privée et de mener leurs affaires personnelles librement.

Certains observateurs soutiennent que le monde a changé — que nous devons accepter une nouvelle réalité dans laquelle les menaces de terrorisme et de crime transnational se font toujours sentir. D'autres sont d'avis que le terrorisme, la menace de violence et l'extrémisme sont des problèmes que les démocraties occidentales combattent avec succès depuis leur apparition. Selon le Commissariat, les menaces de terrorisme et le crime organisé, plutôt que de diminuer l'importance des questions liées à la vie privée, intensifient la nécessité de les prendre en considération. La juge en chef du Canada a mentionné il y a à peine plus d'un an :

> *L'un des effets les plus destructeurs du terrorisme, c'est sa capacité de provoquer des réactions qui sapent les valeurs démocratiques fondamentales sur lesquelles sont fondés nos pays démocratiques. La crainte et la colère suscitées par le terrorisme peuvent amener des dirigeants à faire la guerre à des cibles qui ne sont pas nécessairement liées à l'incident terroriste lui-même. Ou encore, elles peuvent conduire des gouvernements à restreindre les libertés civiles et à recourir à des tactiques, telle la torture, qu'ils dénonceraient normalement — tactiques qui, avec le recul, ne s'avéreront peut-être pas nécessaires ou justifiables*[3].

L'avertissement de la juge en chef fait ressortir le besoin de surveiller efficacement et de réévaluer régulièrement les programmes de lutte contre le terrorisme et de sécurité nationale. La confiance et la cohésion sociale sont peut-être les premières victimes lorsque les gens abandonnent une partie de leur vie privée en faveur de leur sécurité, ou vice-versa. Le lien de confiance entre les citoyens et leurs voisins ainsi qu'entre les citoyens et l'État dépend d'une compréhension mutuelle ou d'un consensus concernant

[3] « Lutter contre le terrorisme tout en préservant nos libertés civiles » — Allocution prononcée par la très honorable Beverley McLachlin, C.P., juge en chef du Canada — adresse URL : http://www.scc-csc.gc.ca/court-cour/ju/spe-dis/bm2009-09-22-fra.asp.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

la nécessité d'assurer la sécurité, de respecter les droits comme celui d'avoir une vie privée et de préserver la société libre et démocratique à laquelle nous tenons tous[4].

Le droit à la vie privée n'est pas simplement un droit individuel ou une liberté civile; c'est un élément essentiel du contrat social entre la population canadienne et son gouvernement. Sans vie privée ni zone de protection entre le gouvernement et les citoyens, la confiance commence à s'effriter[5]. La confiance mutuelle entre l'État et les citoyens est essentielle à une bonne gouvernance. Autrement, un sentiment d'aliénation et d'inégalité commence à se répandre. Dans ces circonstances, aucun programme de sécurité publique n'est viable ou efficace à long terme. En effet, lorsque la confiance des citoyens atteint un niveau plancher, de telles mesures de sécurité peuvent être affaiblies, ignorées, contournées ou — dans les pires des cas — combattues passivement ou activement.

Le droit à la vie privée n'est pas simplement un droit individuel ou une liberté civile; c'est un élément essentiel du contrat social entre la population canadienne et son gouvernement. Sans vie privée ni zone de protection entre le gouvernement et les citoyens, la confiance commence à s'effriter.

L'évolution rapide des nouvelles technologies représente un défi important pour la protection de la vie privée. Les outils, les dispositifs et les systèmes en ligne du 21e siècle fournissent aux organismes gouvernementaux une énorme capacité d'acquisition et d'analyse de l'information. Dans un monde où la plupart des communications électroniques sont consignées, où chaque transaction est enregistrée, les citoyens et les gouvernements doivent travailler davantage pour veiller à ce que l'autonomie et les droits individuels ne soient pas compromis. Au cours de la dernière décennie, des pays du monde entier ont adopté une série de nouvelles lois en matière de sécurité pour acquérir, analyser et exploiter l'information transmise sur ces réseaux numériques[6]. La technologie évolue bel et bien; les menaces aussi. Toutefois, notre façon de réagir à ces changements impose la nécessité d'un cadre de protection qui prend l'initiative de l'action pour faire en sorte que nos valeurs fondamentales comme la protection de la vie privée soient maintenues.

---

[4] Voir également Daniel J. Solove, « Digital dossiers and the dissipation of Fourth Amendment privacy » dans *Southern California Law Review,* no 75 (2002), p. 1083-1167, adresse URL : http://ssrn.com/abstract=313301.

[5] Priscilla M. Regan, dans un ouvrage intitulé « *Legislating Privacy: Technology, Social Values and Public Policy* » publié en 1995, mentionne que la vie privée favorise la confiance, la cohésion sociale et la solidarité; elle n'est pas seulement un droit individuel ou une liberté civile.

[6] Le document d'information du Commissariat intitulé « Pouvoirs de surveillance, de perquisition ou de saisie élargis par des lois récentes au Canada, au Royaume-Uni, en France et aux États-Unis » (Ottawa, 2009) donne un aperçu des récentes modifications législatives — adresse URL : http://www.priv.gc.ca/parl/2009/parl_bg_090507_f.cfm.

Un cadre analytique en matière de protection de la vie privée et de sécurité

Les décideurs font souvent valoir qu'ils ont du mal à prendre pied dans le contexte de la protection de la vie privée et de la sécurité, et que ces nouvelles situations remettent toujours en question les notions établies[7]. Une série de cadres normatifs, d'instruments stratégiques, de lois et de cas de jurisprudence ont été adoptés afin de redéfinir les bases de la protection de la vie privée :

- adoption de la *Loi sur la protection de la vie privée* (1974) qui a mené à la création de la partie VI du *Code criminel* pour réglementer l'écoute téléphonique;
- adoption de la *Loi canadienne sur les droits de la personne* (1977) qui a établi la vie privée en tant que droit fondamental reconnu par la loi et mené à la création du poste de commissaire à la protection de la vie privée;
- adoption de la *Charte canadienne des droits et libertés* (1982);
- débat entourant la *Loi sur la protection des renseignements personnels* du gouvernement fédéral, adoption de celle-ci et établissement administratif du Commissariat à la protection de la vie privée du Canada (1983);
- causes repères en matière de protection de la vie privée tels les arrêts *Oakes* (1986), *Ruby* (2002) et *Tessling* (2004);
- adoption de la loi sur la protection de la vie privée dans le secteur privé au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (2000), qui s'inspire des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'Organisation de coopération et de développement économiques (OCDE);
- application élargie de la gouvernance en matière de protection de la vie privée à toutes les organisations fédérales canadiennes en vertu de la *Loi fédérale sur la responsabilité* (2006).

Chacun de ces jalons dans le traitement et la réglementation des renseignements personnels a façonné notre compréhension de ceux-ci et des situations où il est raisonnable de s'attendre à ce que ces renseignements demeurent privés.
Ces deux concepts de base sont abordés ci-dessous; ils sont suivis d'un aperçu de la façon dont toute nouvelle proposition en matière de sécurité — loi, programme gouvernemental ou initiative réglementaire — peut faire l'objet d'un examen systématique de ses conséquences sur la protection de la vie privée.

Qu'est-ce qu'un « renseignement personnel »?

L'article 3 de la *Loi sur la protection des renseignements personnels* définit les « renseignements personnels » comme étant « [l]es renseignements, quels que soient leur forme et leur support, concernant un individu identifiable », à l'exception des coordonnées professionnelles de cette personne (p. ex. nom, titre, adresse commerciale ou numéro de téléphone d'un employé au sein d'une organisation). Cette définition est

[7] Forum des politiques publiques, *Le régime fédéral sur la protection de la vie privée — Série de tables rondes — Rapport des résultats* (mars 2008), p. 10-12.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

délibérément vaste afin d'assurer une plus grande protection de la vie privée, et les tribunaux canadiens ont généralement hésité à la circonscrire. Par exemple, les tribunaux canadiens ont déterminé que les numéros d'assurance sociale, les adresses de courriel et les messages électroniques, les achats des consommateurs, les historiques de transactions et de services ainsi que les renseignements sur les comptes et les adhésions des consommateurs font partie des renseignements personnels. Des renseignements peuvent également être considérés comme « personnels » même s'ils sont accessibles au public. La diffusion de renseignements personnels dans le domaine public dans un but déterminé n'annule pas toutes les restrictions relatives à la collecte, à l'utilisation ou à la communication systématiques à d'autres fins.

L'apparition de nouvelles technologies a élargi le concept de renseignements personnels. Ceux qui utilisent la nouvelle génération d'appareils de communication produisent constamment des données sur eux-mêmes. Par conséquent, même les données biométriques (comme les empreintes digitales et vocales), les séquences vidéo numériques (comme celles du lieu de résidence ou des déplacements d'une personne), les adresses de protocole Internet (IP) ou les données de géolocalisation (p. ex. les points de localisation recueillis à partir d'une étiquette d'identification par radiofréquence [IRF] ou d'un système de positionnement global [GPS]) pourraient être considérées comme des renseignements personnels dans certaines circonstances. Bien que ces données de localisation granulaires ambiantes n'en disent pas beaucoup au sujet d'une personne lorsqu'elles sont prises isolément, il y a manifestement un enjeu lié à la protection de la vie privée lorsque ces flux de données sont produits en continu ou combinés avec d'autres données. En effet, ces pistes ou ces émissions de données peuvent être très révélatrices si elles sont recueillies à grande échelle, rassemblées dans des profils personnels et analysées en vue d'établir des tendances ou des indications sur les comportements.

L'apparition de nouvelles technologies a élargi le concept de renseignements personnels. Ceux qui utilisent la nouvelle génération d'appareils de communication produisent constamment des données sur eux-mêmes.

Quand y a-t-il attente raisonnable en matière de vie privée?

Bien que l'expression « vie privée » ne figure pas dans la *Charte*, celle-ci protège divers droits et intérêts en matière de vie privée. Par exemple, des intérêts liés à la protection de la vie privée sont notamment associés au droit à la vie, à la liberté et à la sécurité de la personne, qui est protégé par l'article 7 de la *Charte* pour ce qui est du contrôle sur sa personne et ses renseignements personnels[8]. La Cour suprême du Canada a laissé entendre que le droit à la vie privée pourrait en lui-même être un principe de justice fondamentale[9], et elle a reconnu que le droit à la vie privée et à la protection des

[8] Voir Stanley A. Cohen, « The Legal Basis of Privacy under the Charter » dans *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (2005), p. 14-19; voir également « Privacy protection under the Charter of Rights and Freedoms » dans *The Law of Privacy in Canada* (2009), p. 2.3 à 2.15.
[9] *R. c. Mills*, [1999] 3 R.C.S. de 668 à 714.

renseignements personnels est un aspect essentiel de la liberté dans une société libre et démocratique.

Certains commentateurs ont indiqué que divers intérêts liés à la vie privée sont protégés par les libertés fondamentales ainsi que par le droit à la liberté de circulation et d'établissement, le droit d'une personne arrêtée à l'assistance d'un avocat, le droit pour un témoin de garder le silence et le droit à la protection contre les témoignages incriminants[10]. Au Canada, la notion d'« attente raisonnable en matière de vie privée » découle de l'interprétation par les tribunaux de l'article 8 de la *Charte*, qui protège les personnes contre les fouilles, les perquisitions ou les saisies abusives lorsqu'il y a une « attente raisonnable en matière de vie privée ». Le juge Lebel indique dans *R. c. Kang-Brown* que « l'art. 8 est devenu, dès les premiers arrêts portant sur son application, un bouclier contre les ingérences injustifiées de l'État dans la vie privée des gens ».

Pour déterminer si les attentes en matière de vie privée d'une personne sont raisonnables dans un cas donné, il faut effectuer une évaluation contextuelle des faits précis relatifs à une fouille particulière, ainsi qu'une appréciation d'éléments subjectifs et objectifs. La jurisprudence a aussi répété à maintes reprises que l'article 8 protège « les personnes et non les lieux ». Le droit à la vie privée au Canada a historiquement été rattaché à la protection des biens[11], mais la jurisprudence canadienne, en ce qui a trait à l'interprétation de l'article 8 de la *Charte*, reconnaît maintenant que les Canadiennes et Canadiens peuvent aussi avoir des attentes en matière de vie privée lorsqu'ils sont dans un lieu public.

Par conséquent, c'est la protection consentie par l'article 8 de la *Charte* et l'interprétation qu'en font les tribunaux qui donnent du poids à la protection de la vie privée des personnes, surtout dans le contexte des initiatives gouvernementales en matière de sécurité. Pour ce qui est des fouilles effectuées par les organismes gouvernementaux, la Cour suprême du Canada a reconnu que l'attente d'une personne en matière de vie privée peut dépendre du lieu, de la nature des renseignements et du lien entre les renseignements et la personne.

En ce qui a trait à cet élément, un critère adopté par la Cour suprême du Canada afin de déterminer si les attentes raisonnables d'une personne en matière de vie privée consiste à demander si les renseignements personnels consultés par le gouvernement comportent « un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État.[12] » À mesure que de nouvelles technologies et de nouvelles pratiques sociales font leur apparition et informent notre conception de la vie privée, elles peuvent également soulever des préoccupations en matière de sécurité; les principes juridiques fondamentaux deviennent donc d'autant plus importants. Enfin,

---

[10] Alain-Robert Nadeau, *Vie privée et droits fondamentaux : étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international* (Scarborough, Ont. : Carswell, 2000) à 106.

[11] Eric H. Reiter, « Privacy and the Charter: Protection of People or Places? » (2009) vol. 88, La revue du Barreau canadien, p. 119-123.

[12] *R. c. Plant* (1990); voir également ce que dit le juge Lamer dans l'affaire *Schreiber c. Canada* (1998) : « la vie privée est non pas un droit se rattachant à des biens, mais plutôt un élément crucial de la liberté individuelle qui commande à l'État de respecter la dignité, l'autonomie et l'intégrité de l'individu. »

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

comme il a été mentionné plus tôt, le contexte est essentiel lorsque les tribunaux déterminent si les attentes des citoyens sont raisonnables en ce qui a trait à la vie privée. Comment les renseignements personnels sont-ils recueillis, par qui, comment et dans quel but?

Toutes ces questions servent à établir le contexte dans lequel la vie privée est envisagée, et elles créent une structure qui sous-tend les renseignements personnels et qui peut être considérée comme une protection ou une menace. L'affaire *Tessling* a relevé l'importance pour les représentants du gouvernement de tenir compte de la « totalité des circonstances[13] ». Cela signifie que, dans le cadre de la conception des programmes de sécurité, il ne faut pas uniquement tenir compte des attentes *subjectives* (c.-à-d. est-ce que les personnes pensent que leurs renseignements ou interactions sont privés dans le contexte proposé?), mais aussi d'éléments objectifs, dont les suivants :

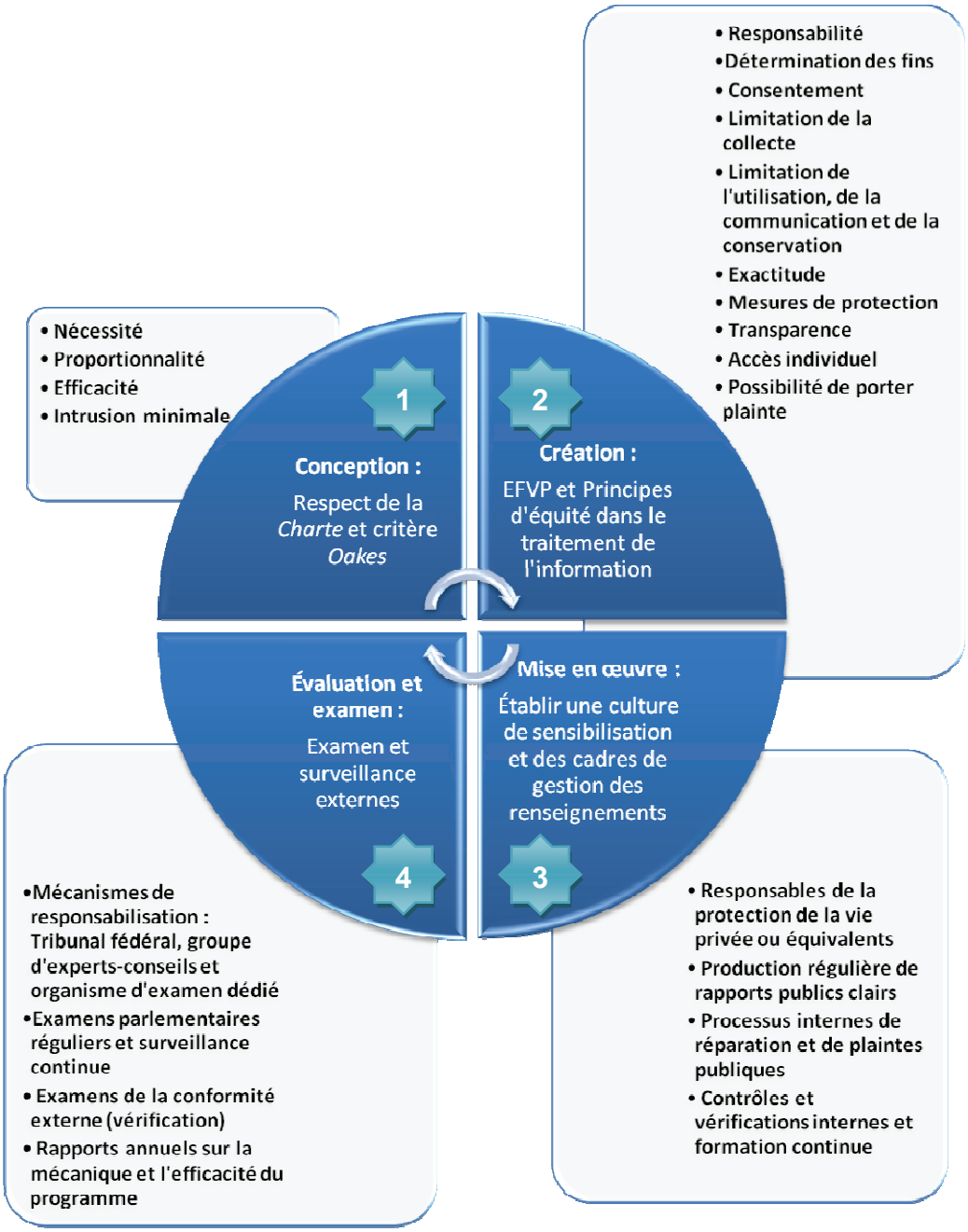
À mesure que de nouvelles technologies et de nouvelles pratiques sociales font leur apparition et informent notre conception de la vie privée, elles peuvent également soulever des préoccupations en matière de sécurité; les principes juridiques fondamentaux deviennent donc d'autant plus importants.

- Les renseignements demandés révèlent-ils le mode de vie d'une personne ou sont-ils des « renseignements biographiques fondamentaux »? — par exemple des pensées et des réflexions personnelles, des opinions politiques, des renseignements sur la santé mentale ou des troubles médicaux;
- La fouille était-elle ouverte ou secrète? — cela dépend si la personne visée savait qu'elle-même et ses biens faisaient l'objet d'un examen approfondi (par exemple dans le cas d'une inspection matérielle ou d'une fouille des lieux justifiée) ou si les agissements ou les communications du citoyen ont été enregistrés en secret;
- Où la surveillance a-t-elle été menée? — dans un lieu totalement public ou un peu à l'abri des regards, par exemple dans un véhicule ou un bureau;
- Les renseignements se trouvaient-ils en possession de la personne ou avaient-ils été abandonnés? — par exemple si les renseignements sont enregistrés sur un appareil personnel protégé par un mot de passe ou, au contraire, tout simplement écrits sur un morceau de papier qui a été jeté;
- Les renseignements étaient-ils entre les mains d'un tiers et considérés comme confidentiels? — entre les mains d'une entreprise de télécommunications, d'un organisme gouvernemental ou encore d'un représentant juridique, par exemple;
- Une technique d'enquête intrusive a-t-elle été utilisée? — par exemple une caméra cachée, un microphone dissimulé, un traceur personnel, un logiciel espion ou une autre méthode cachée;
- La méthode de surveillance serait-elle jugée objectivement raisonnable dans les circonstances?

[13] *R. c. Tessling [2004] 3 R.C.S. 432* : « Peu de choses revêtent autant d'importance pour notre mode de vie que l'étendue du pouvoir conféré à la police d'entrer dans la maison d'un citoyen canadien, de porter atteinte à sa vie privée et même à son intégrité corporelle sans autorisation judiciaire. »

La protection de la vie privée dès le départ : quatre étapes à prendre en compte

L'élaboration et la mise en œuvre de programmes et de politiques touchant la sécurité suivent quatre grandes étapes — la conception, la création, la mise en œuvre et l'évaluation. Certains facteurs doivent être pris en considération à chacune de ces étapes pour veiller à ce que la vie privée soit respectée et que le tout soit bien documenté (comme c'est le cas dans les évaluations des facteurs relatifs à la vie privée). Ces grandes étapes sont présentées ci-dessous :



priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Étape 1 : « Établir le bien fondé » — Conformité à la Charte *et à l'arrêt* Oakes

À la suite de la promulgation de la *Charte canadienne des droits et libertés* en 1982, la Cour suprême du Canada a établi un critère méthodologique pour déterminer si la violation d'un droit de la *Charte* est justifiée dans une société libre et démocratique. Comme il émane de l'arrêt *R. c. Oakes*, ce critère est généralement connu sous le nom de critère *Oakes*[14]. Il exige ce qui suit :

- **La nécessité :** il doit y avoir une nécessité clairement définie, liée à une préoccupation sociétale pressante, en vue du recours à la mesure (en d'autres termes, un problème substantiel et imminent que l'on tente de régler par l'entremise de la mesure de sécurité).

- **La proportionnalité :** la mesure (ou l'exécution précise d'un pouvoir envahissant) doit être minutieusement ciblée et personnalisée afin d'être raisonnablement proportionnelle à l'atteinte à la vie privée (ou à tout autre droit) de la personne visée.

- **L'efficacité :** on doit démontrer que la mesure est empiriquement efficace en vue de régler le problème et être clairement associée à la résolution du problème.

- **Une intrusion minimale :** la mesure doit être l'option la moins envahissante (en d'autres termes, il faut s'assurer que toutes les autres options d'enquête moins envahissantes ont été épuisées).

L'importance de l'objectif, sa justification sous-jacente ainsi qu'une tentative claire de minimiser les effets sociaux de toute intrusion sont tous des éléments qui doivent faire partie intégrante de cette analyse. Bien qu'il ait été conçu pour déterminer si une apparence de violation de la *Charte* est justifiée en application de l'article 1 de celle-ci, le critère *Oakes* fournit un cadre utile pour analyser la viabilité d'une nouvelle initiative de sécurité proposée.

À l'instar du critère *Oakes*, les cas de jurisprudence qui abordent précisément les limites des pouvoirs de la police peuvent servir dans le cadre d'une évaluation de la légitimité des initiatives de sécurité qui ont une incidence sur la vie privée[15]. Dans l'arrêt *R. c. Godoy*, par exemple, la Cour suprême a statué :

> *Bien que chacun ait droit au respect de la vie privée dans l'intimité de son foyer tenu pour inviolable, l'intérêt que présente pour le public le maintien d'un système d'intervention d'urgence efficace est évident et suffisamment important pour que puisse être commise une atteinte au droit à la vie privée de l'occupant. Cependant, l'atteinte doit se limiter à la protection de la vie et de la sécurité; les agents de police ne sont pas autorisés en plus à fouiller les lieux ni à s'immiscer autrement dans la vie privée ou la propriété de l'occupant.*[16]

14 *R. c. Oakes* [1986] 1 S.C.R. 103.
15 Voir notamment *R. c. Waterfield,* [1963] 3 All E.R. 659; *R. c. Stenning,* [1970] S.C.R. 631; *Dedman c. Sa Majesté,* [1985] 2 S.C.R. 2.
16 *R. c. Godoy*, [1999] 1 S.C.R. 311.

La Cour a déterminé que la justification de l'utilisation des pouvoirs de la police et l'interruption des libertés individuelles reposent sur un certain nombre de facteurs, dont la mission précise accomplie par la police, la mesure dans laquelle l'interruption des libertés individuelles est nécessaire pour accomplir la mission, l'importance de la mission relativement au bien collectif, la nature de la liberté mise en cause, et la nature et la portée de l'interruption[17].

Évaluer les initiatives en matière de sécurité selon la jurisprudence au sujet des apparences de violation des intérêts d'une personne peut aider à faire en sorte que le mandat légal d'un programme est bien ciblé, que les pouvoirs sont adaptés de manière appropriée et que l'incidence du programme sur les droits et libertés établis est limitée. Cela établit également un critère en vue de déterminer si l'atteinte à un droit fondamental peut être justifiée de manière raisonnable. Les organismes de sécurité gouvernementaux qui ne prendraient pas les mesures nécessaires pour discuter de leur approche, documenter celle-ci et montrer qu'elle est équilibrée et réfléchie relativement à ces aspects de la collecte de renseignements s'exposent aux critiques des organismes d'examen, des intervenants du domaine du commerce, des élus et du grand public canadien.

Les organismes de sécurité gouvernementaux qui ne prendraient pas les mesures nécessaires pour discuter de leur approche, documenter celle-ci et montrer qu'elle est équilibrée et réfléchie relativement à ces aspects de la collecte de renseignements s'exposent aux critiques des organismes d'examen, des intervenants du domaine du commerce, des élus et du grand public canadien.

Étape 2 : « Définir les balises » — Principes relatifs à l'équité dans le traitement de l'information

Après l'évaluation de la pertinence de la collecte des renseignements à l'aide des critères établis dans *Oakes* ou une analyse similaire, un deuxième ensemble de questions opérationnelles peut être examiné pour veiller à ce que les renseignements personnels soient traités et protégés adéquatement. Dans le secteur public, cet examen correspond généralement à l'évaluation des facteurs relatifs à la vie privée (EFVP) qui est à la vie privée ce que les évaluations de la menace et des risques (EMR) sont aux enjeux de sécurité. Les deux exercices font en sorte que le droit à la vie privée et la sécurité des Canadiennes et des Canadiens sont soigneusement pris en compte au moment de concevoir un nouveau programme ou service fédéral.

À cette étape-ci, les *Principes relatifs à l'équité dans le traitement de l'information*, largement acceptés, peuvent s'appliquer afin de veiller à ce que l'architecture détaillée d'une technique ou d'un programme gouvernemental particulier soit évaluée et élaborée en tenant compte de la protection de la vie privée. Ces principes servent de fondement aux lois sur la protection de la vie privée de nombreux pays (y compris à la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada) :

17 *R. c. Godoy*, [1999] 1 S.C.R. 311, par. 18.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

- **Responsabilité** — veiller à ce qu'une personne soit activement responsable des renseignements et mette en place des politiques et des procédures appropriées;
- **Détermination des fins de la collecte des renseignements** — préciser pourquoi les renseignements personnels sont recueillis;
- **Consentement** — la personne visée doit consentir à une utilisation de ses renseignements personnels autre que celle visée par les fins de la collecte ou en dehors de certaines exemptions limitées;
- **Limitation de la collecte** — recueillir uniquement les renseignements pertinents nécessaires en vue d'atteindre l'objectif en matière de sécurité et employer seulement des moyens légaux et équitables;
- **Limitation de l'utilisation, de la communication et de la conservation** — imposer des restrictions rationnelles et appropriées relatives à la communication de renseignements de nature délicate à des tiers, limiter l'utilisation ou la communication à des fins précises et limiter le temps de conservation des données requis pour atteindre l'objectif;
- **Exactitude** — veiller à ce que les renseignements personnels soient suffisamment précis, complets et à jour pour minimiser les risques que des décisions inappropriées soient prises sur une personne;
- **Mesures de sécurité** — protéger les renseignements personnels à l'aide de mesures de sécurité adaptées au degré de sensibilité des renseignements;
- **Transparence** — faire connaître les politiques et les pratiques en matière de vie privée d'un organisme en fournissant de l'information aux citoyens;
- **Accès aux renseignements personnels** — permettre aux personnes de consulter leurs renseignements personnels, d'en contester l'exactitude et l'intégralité et de les modifier au besoin;
- **Possibilité de porter plainte à l'égard du non-respect des principes** — établir une procédure de plainte.

Ces principes sont des éléments concrets en matière de protection de la vie privée dont tiendront compte les planificateurs ou les décideurs au cours des premières étapes de l'élaboration de toute nouvelle initiative touchant la sécurité publique. Les principes bien établis de la protection de la vie privée, comme ils sont énoncés dans de nombreuses lois sur la protection des données, offrent un filtre visant à traiter l'enjeu de la collecte excessive de données.

Ces principes aideront à faire en sorte que les programmes de sécurité publique soient bien définis et structurés adéquatement. Certains organismes gouvernementaux responsables de la sécurité publique ont adopté ces pratiques de protection de la vie privée et ces principes relatifs à l'équité dans le traitement de l'information pour améliorer leur transparence et leur efficience (l'annexe A, « Trois études de cas sur la protection de la vie privée et la sécurité » fournit des exemples de mesures de contrôle et de vérification précises). Soulignons que le cycle de traitement des renseignements et la procédure de classification militaire comprennent des ressemblances et des antécédents manifestes liés à bon nombre de ces principes généraux relatifs à la protection des données.

Tout au long du 20e siècle, les autorités responsables de la sécurité et du renseignement de partout au monde ont utilisé beaucoup de ressources en vue de trouver des façons de recueillir un plus grand nombre de données provenant de sources très disparates, plus rapidement. Comme tous les analystes et décideurs gouvernementaux, les organismes de sécurité étaient souvent embêtés par les

exigences techniques, l'effectif nécessaire et les problèmes de communication lorsqu'il fallait recueillir et analyser des renseignements suffisamment rapidement pour les utiliser dans le contexte de la sécurité nationale. Il était toujours considéré comme un avantage de disposer d'une quantité plus importante de renseignements.

Toutefois, les progrès impressionnants réalisés dans le domaine des technologies de l'information et des communications ont grandement accéléré et raffiné le processus d'acquisition de renseignements, ainsi que le nombre de sources d'information à la disposition du gouvernement. Le défi consistait plutôt à isoler ce qui était nécessaire, important et révélateur au sujet des menaces à la sécurité parmi une immense quantité de données diffusées quotidiennement. Les forces de sécurité sont maintenant très efficaces pour amasser les pièces du puzzle; le défi, c'est de les assembler.

Les technologies des communications ont grandement accéléré et raffiné le processus d'acquisition de renseignements du gouvernement. Le défi consiste à isoler ce qui est nécessaire, important et révélateur au sujet des menaces à la sécurité parmi une immense quantité de données diffusées quotidiennement.

Les principes relatifs à la protection de la vie privée ne doivent pas être perçus sans préambule comme des obstacles à la collecte ou à l'échange de renseignements, mais plutôt comme un puissant moyen de cibler l'analyse. Une approche minimaliste — inhérente à la protection de la vie privée — peut être un modèle utile pour cibler la collecte et l'utilisation des renseignements. Ainsi, les enquêtes et les renseignements sont rationalisés et focalisés sur les questions liées à l'atteinte des objectifs en matière de sécurité publique.

Étape 3 : « Exécuter le programme » — Intégrer la protection de la vie privée à la gestion de l'information

Après avoir intégré les mesures de protection de la vie privée décrites ci-dessus à l'architecture de base d'un programme, l'organisation doit assurer sa conformité en élaborant des mécanismes internes. Ceux-ci devraient constituer le troisième élément ou la troisième étape de l'établissement de mesures de protection au sein des organisations, lorsqu'un programme de sécurité passe de l'étape de la conception initiale aux opérations courantes[18]. Les mécanismes internes doivent être considérés comme des moyens de maintenir le souci du respect de la vie privée, par exemple :

- ❑ rôles et responsabilités organisationnels clairs pour le traitement des renseignements personnels, y compris un examen régulier aux fins d'exactitude et de pertinence continue des renseignements personnels de nature délicate;
- ❑ documentation accessible en langage clair sur les politiques et pratiques en matière de protection de la vie privée;

[18] Pour une discussion plus approfondie et des recommandations à ce sujet, voir *Cadres de gestion de la protection de la vie privée de certaines institutions fédérales — Rapport de vérification de la commissaire à la protection de la vie privée du Canada* (2009), www.priv.gc.ca/information/pub/ar-vr/pmf_20090212_f.pdf.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

- ❑ solide capacité de vérification interne en ce qui a trait aux questions relatives à la protection de la vie privée, particulièrement dans les domaines de l'accès, des mesures de sécurité et de l'échange de renseignements;
- ❑ ententes détaillées en place pour les cas d'échange de renseignements personnels;
- ❑ présentations régulières de rapports destinés au public et publication de renseignements sur les évaluations des facteurs relatifs à la vie privée (EFVP);
- ❑ processus internes simples en vue du traitement et du signalement des plaintes, des problèmes ou des atteintes à la protection des données possibles;
- ❑ formation continue en matière de protection de la vie privée offerte tant au personnel de première ligne qu'à la direction;
- ❑ responsabilité à l'échelle de la haute direction concernant la gestion des éléments des programmes relatifs à la protection de la vie privée, y compris la nomination des responsables de la protection de la vie privée.

La Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor administre un ensemble complet de politiques, de lignes directrices et de pratiques exemplaires dans ce domaine. Il est essentiel d'y faire référence en vue de concevoir avec soin tout système ou programme qui traitera de renseignements personnels au nom du gouvernement du Canada (voir l'annexe B, « Politique, directives et documents d'orientation du Conseil du Trésor relatifs à la protection de la vie privée »).

La Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor administre un ensemble complet de politiques, de lignes directrices et de pratiques exemplaires.

Étape 4 : « Calibrer le système » — Examen externe et surveillance

Les programmes de sécurité publique permettent souvent de recueillir et d'utiliser des renseignements personnels à très grande échelle. Dans une société démocratique, ces programmes doivent être soumis à des examens externes indépendants, proportionnés à la portée des pouvoirs consentis et aux atteintes possibles à la vie privée. Une tendance se dégage des nombreux examens législatifs, enquêtes et rapports sur le système canadien de sécurité nationale : de mauvaises pratiques de traitement de l'information, des mécanismes de reddition de comptes disparates et une surveillance limitée peuvent mener à des erreurs tragiques et coûteuses dans le cadre des opérations relatives à la sécurité nationale[19]. En cette époque de réseaux d'échange de renseignements stratégiques, il nous faut des réseaux d'examen et de surveillance.

Les mécanismes d'examen et de surveillance comprennent notamment un processus systématique de traitement des plaintes et des préoccupations du public, l'application

[19] Le Canada a mené de nombreuses enquêtes publiques pour les questions de sécurité : les enquêtes de Wells (1966) et de Spence (1966) sur les tactiques de chasse aux agents d'infiltration communistes de la GRC, la Commission Mackenzie (1969) qui recommande de détacher les activités de sécurité de l'État du mandat de la GRC, la Commission Marin concernant les plaintes à la GRC (1974) et les Commissions d'enquête Keable et McDonald (1981) qui se penchent sur les activités de la GRC au Québec visant à surveiller et à miner les souverainistes. Plus récemment, nous avons connu les enquêtes O'Connor (2006), Iacobucci (2008) et Major (2009), toutes axées sur une facette ou une autre de la structure de sécurité nationale du Canada.

d'une méthode clairement articulée à des fins d'appel et de réexamen en cas de problèmes ainsi qu'un examen périodique externe effectué par les parlementaires et des organismes de surveillance à qui on a confié ce mandat. Tous ces mécanismes de contrôle sont importants pour faire en sorte que les mesures de protection de la sécurité tiennent compte des droits et les intègrent. Les programmes de sécurité publique ne peuvent être exemptés de ces mécanismes de légitimité. Au contraire, les pouvoirs qu'ils confèrent peuvent être si vastes et discrétionnaires qu'ils nécessitent une surveillance en conséquence. En outre, un mécanisme clair d'examen et de recours indépendants, doté de pouvoirs suffisants et de ressources adéquates, ajoute foi et crédibilité à tout programme ou projet.

> En cette époque de réseaux d'échange de renseignements stratégiques, il nous faut des réseaux d'examen et de surveillance.

Divers mécanismes d'examen externe et de surveillance peuvent être adoptés, notamment les examens parlementaires quinquennaux des mesures législatives et une plus grande participation des comités de la Chambre des communes et du Sénat dans l'examen des organismes et programmes de sécurité publique, des organismes d'examens externes spécialisés, et une transparence accrue grâce à une meilleure utilisation des rapports annuels et d'autres processus d'établissement de rapports. Certains de ces mécanismes servent déjà. Par exemple, le Comité de surveillance des activités de renseignement de sécurité (CSARS) revoit en détail les activités du Service canadien du renseignement de sécurité (SCRS) et le commissaire du Centre de la sécurité des télécommunications (CST) revoit en détail les activités du CST; dans les deux cas, on fait référence explicitement à la protection de la vie privée.

En dernier recours, de nombreuses organisations imposent des pénalités précises à ceux qui accèdent sans autorisation à des systèmes qui comprennent des renseignements délicats ou qui font un usage indu des renseignements personnels. La GRC et d'autres forces policières du Canada, par exemple, ont établi un ensemble de règlements qui permettent à leurs organismes d'imposer des amendes et de punir ou même de suspendre des agents qui ne traitent pas correctement des sources et des systèmes sécurisés ou qui consultent des renseignements personnels de façon inacceptable. Dans le même ordre d'idées, le *Code criminel* impose des interdictions encore plus sévères et prévoit un emprisonnement maximal de cinq ans à quiconque intercepte une communication privée sans autorisation[20].

Rappelons en terminant que la présentation de rapports publics (par exemple les rapports annuels relatifs à la *Loi sur la protection des renseignements personnels* ou les rapports ministériels sur le rendement) est un autre mécanisme qui protège la vie privée en démontrant les mesures prises et pour protéger la vie privée et leur efficacité, en ciblant les lacunes, en examinant les incidents, en analysant les tendances et en recommandant des améliorations aux processus et aux systèmes. Le CSARS et le commissaire du CST, par exemple, doivent soumettre à leurs ministres respectifs des rapports annuels qui seront présentés au Parlement. Le rapport concernant le SCRS comprend même une analyse du système de mandats du SCRS et l'utilisation de la

[20] *Code criminel,* Partie VI — Atteintes à la vie privée, article 184.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

surveillance; Sécurité publique Canada dépose un rapport annuel similaire sur l'utilisation de la surveillance électronique.

Au Canada, comme dans la plupart des autres pays, les opérations du gouvernement concernant la sécurité sont en grande partie effectuées en secret. Ces exceptions peuvent être justifiées par des raisons valides. Un certain niveau d'autonomie, et même de tromperie, est nécessaire pour réaliser un travail délicat et caché. Toutefois, lorsque des erreurs sont découvertes, la complexité de ces opérations et le secret qui les entoure peuvent faire en sorte que les recours publics d'envergure sont difficiles et, dans certains cas, presque impossibles. Il est donc essentiel de contrebalancer ce besoin de confidentialité à l'aide de mécanismes d'examen et de mesures de reddition de comptes solides[21].

[21] Pour en savoir plus sur la surveillance et les examens proactifs dans le contexte de la sécurité, consulter le document intitulé *Droits et réalité : augmenter la surveillance des programmes en matière de sécurité nationale du Canada* (Ottawa, 2009) adresse URL : http://www.priv.gc.ca/parl/2009/parl_sub_090507_f.pdf.

Conclusion : vie privée, sécurité et les enjeux pour la démocratie

Quels sont donc les enjeux en cause au moment où les décideurs et les législateurs doivent se pencher sur l'intégration du droit à la vie privée dans les initiatives de sécurité publique? Quelles sont les répercussions pour le Canada? La question de la confiance est la plus importante pour le gouvernement. La confiance entre les citoyens et leurs voisins de même qu'entre les citoyens et l'État repose sur une compréhension mutuelle de la protection de la vie privée, de sa valeur en tant que droit de la personne et du bien commun.

Les gouvernements sont préoccupés à juste titre par les coûts associés à l'évaluation adéquate des répercussions sur la vie privée des initiatives en matière de sécurité. Pourtant, l'ensemble des pays dépense désormais chaque année des dizaines de milliards de dollars pour la collecte, l'analyse et le partage de renseignements utiles à des fins de sécurité. Les systèmes et les analystes du gouvernement peuvent sonder pratiquement chaque aspect de la vie des personnes; ces mesures s'avèrent expansives et coûteuses, et l'effort, intensif et envahissant.

Certains aspects de l'équation sont difficilement quantifiables. Ces mesures de sécurité sont-elles proportionnées dans leur caractère envahissant? Sont-elles efficaces à contrer la menace qu'elles cherchent à atténuer? Sont-elles nécessaires en bout de ligne, ou une autre tactique, approche ou logique pourrait-elle convenir davantage? Comme la politique canadienne en matière de sécurité nationale l'énonce clairement d'entrée de jeu, l'un des plus importants défis pour notre démocratie dans sa lutte contre les menaces à la sécurité consiste à s'assurer d'éviter qu'« on érode par inadvertance les libertés et les valeurs que nous sommes déterminés à défendre[22] ». En conclusion, le présent document vise principalement à fournir une référence dans le contexte changeant de la sécurité de manière à ce que le droit fondamental à la vie privée soit protégé.

[22] Gouvernement du Canada, *Protéger une société ouverte : la politique canadienne de sécurité nationale* (Ottawa, 2004), p. 3, adresse URL : http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-fra.pdf.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Remerciements

Le Commissariat tient à remercier tout spécialement les deux universitaires qui ont dirigé ce projet à l'étape de l'examen et de la consultation, soit Karim Benyekhlef, directeur du Centre de recherche en droit public à la Faculté de droit de l'Université de Montréal, et Arthur Cockfield, professeur agrégé à la Faculté de droit de l'Université Queen's. Leur soutien et leur objectivité nous ont été d'une aide inestimable.

Le Commissariat souhaite également remercier très sincèrement un groupe dévoué d'experts, de chercheurs et d'observateurs pour avoir partagé leurs commentaires et leurs expériences. Tous ont investi temps et énergie dans l'examen des idées énoncées dans le présent document et se sont réunis afin de débattre de sa forme finale et de formuler des commentaires à ce sujet. Nous désirons souligner leur contribution.

Parmi ces examinateurs, on retrouve :

- L'honorable Perrin Beatty
- Pierre-Yves Borduas
- Karine Côté-Boucher
- Horst Intscher
- Edna Keeble
- Le Canadian Council on American-Islamic Relations (CAIR-CAN)

Enfin, un merci tout spécial à Chris Prince, analyste des politiques stratégiques au Commissariat à la protection de la vie privée du Canada, pour son travail acharné au cours de l'élaboration du rapport et des consultations.

Annexe A : Trois études de cas sur la protection de la vie privée et la sécurité

Étude de cas n^{o} 1 : Le Programme de protection des passagers (liste des personnes interdites de vol)

La mission de Transports Canada consiste à élaborer et à administrer des politiques, des règlements et des services afin d'offrir le meilleur réseau de transport au Canada. Le Programme de protection des passagers (PPP) vise à empêcher les individus qui présentent une menace immédiate pour la sécurité aérienne de monter à bord d'un aéronef dans un aéroport canadien désigné. En s'appuyant sur les informations reçues des organismes de sécurité et de renseignements canadiens et internationaux, Transports Canada dresse et maintient la Liste des personnes précisées (LPP). Lorsqu'un transporteur aérien établit qu'une personne souhaitant monter à bord d'un aéronef figure sur la LPP et que cela est par la suite confirmé par Transports Canada, on doit lui refuser l'embarquement.

Les renseignements personnels gérés dans le cadre du PPP comprennent des renseignements secrets sur des personnes précises fournis par des organismes de sécurité et de renseignements canadiens ou étrangers; des renseignements sur les personnes qui figurent sur la LPP (noms, pseudonymes, sexe et date de naissance); des renseignements sur les personnes dont les noms pourraient correspondre à un de ceux qui se trouvent sur la LPP transmise par les transporteurs aériens à Transports Canada; des renseignements pour appuyer les demandes de réexamen.

Transports Canada a présenté au Commissariat une évaluation des facteurs relatifs à la vie privée (EFVP) afin de s'assurer que la protection de la vie privée soit intégrée au cœur du PPP. Par exemple, Transports Canada mentionne son intention de restreindre l'utilisation des renseignements personnels liés au Programme à une seule fin imposée par la loi, c'est-à-dire de diminuer les menaces contre la sécurité des transports.

Critère en quatre parties : nécessité, efficacité, proportionnalité et autres solutions possibles

Dans son examen de l'EFVP, le Commissariat s'est dit préoccupé par les risques qu'un projet de liste de personnes interdites de vol posent pour la protection de la vie privée. Pour ce qui est de la proportionnalité, le Commissariat est d'avis que le PPP peut enfreindre gravement le droit à la vie privée et la liberté de mouvement des passagers aériens au Canada. Le Commissariat soutient également qu'il y a des risques d'une mauvaise utilisation des renseignements. Le Commissariat craint surtout que les personnes qui sont ajoutées à la liste par erreur ou qui sont considérées à tort comme des menaces subissent de graves conséquences négatives allant des désagréments et des retards à un interrogatoire très envahissant, une fouille et une détention en raison d'une correspondance avec la liste.

Quant à la nécessité et à l'efficacité, le Commissariat soutient qu'aucune étude ou analyse de Transports Canada ne démontre que la LPP est un outil utile et efficace pour améliorer la sécurité du système de transport aérien au Canada. Le Commissariat a

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

ensuite recommandé que Transports Canada embauche une tierce partie indépendante et expérimentée pour évaluer le PPP et son efficacité.

Principes relatifs à l'équité dans le traitement de l'information

Responsabilité — Transports Canada a remis au Commissariat une copie des protocoles d'entente (PE) signés avec le SCRS, la GRC et des transporteurs aériens. Bien que ces PE abordent un grand nombre de questions, ils contiennent très peu de dispositions sur la protection de la vie privée et des données. Le Commissariat recommande que des dispositions soient ajoutées pour préciser les méthodes servant à échanger les renseignements personnels, les mesures administratives et techniques ainsi que les mesures de sécurité à prendre pour protéger les renseignements, les exigences concernant la conservation et le retrait des renseignements personnels qui sont échangés et l'obligation de vérifier régulièrement la gestion des renseignements.

Limitation de l'utilisation, de la communication et de la conservation — Au moment de la rédaction de son EFVP, Transports Canada n'avait pas encore établi un cadre de conservation et de retrait des renseignements personnels liés au Programme. Le Commissariat a recommandé au Ministère d'en élaborer un avant que le Programme entre en vigueur. Le Commissariat était aussi préoccupé par l'échange de renseignements qui se trouvent sur la LPP avec des gouvernements et des autorités policières étrangères, car il craignait — et craint encore — que ces renseignements soient utilisés à d'autres fins.

Exactitude — Le Commissariat a manifesté son inquiétude que des noms soient ajoutés à la LPP par erreur et que des « faux positifs » soient interdits de vol. Il a notamment recommandé que Transports Canada : élabore et documente des politiques et des procédures pour faire en sorte que les critères de sélection des personnes ajoutées à la LPP soient solides et appliqués uniformément par les organismes de sécurité qui participent au processus; examine périodiquement les normes et les critères utilisés pour ajouter des noms à la LPP; mette en place des procédures appropriées pour qu'une personne soupçonnée par un transporteur aérien de figurer sur la LPP soit bel et bien la personne indiquée sur la liste; élabore et documente des procédures pour aviser les partenaires (le SCRS et la GRC) qu'un nom a été retiré de la liste à la suite d'une procédure menée dans le cadre du mécanisme de réexamen.

Mesures de sécurité — L'examen de l'EFVP a révélé que certaines procédures de sécurité précises n'avaient pas encore été documentées, y compris les procédures d'urgence dans l'éventualité d'une communication non autorisée de renseignements personnels. Transports Canada a réagi en ajoutant des procédures et des exigences en matière de sécurité aux PE signés avec des transporteurs aériens et en élaborant des procédures de sécurité et d'urgence à l'intention des employés de Transports Canada. Le Commissariat était satisfait du plan d'intervention en cas d'incident lié à la protection des renseignements personnels, car il fournissait une orientation adéquate au personnel de Transports Canada en cas d'atteintes à la protection des renseignements personnels.

Transparence — Au moment de la rédaction de son EFVP, Transports Canada n'avait pas créé de fichiers de renseignements personnels (FRP) liés au PPP à verser dans Info Source. Transports Canada a par la suite rédigé deux FRP : un pour les renseignements personnels conservés dans le cadre du PPP et l'autre pour les

renseignements personnels détenus par le Bureau de réexamen. Toutefois, les FRP ne décrivent pas tous les usages compatibles possibles des renseignements personnels recueillis. Aux fins de transparence publique, le Commissariat a recommandé que les deux FRP soient révisés de façon à mentionner tous les usages compatibles qui peuvent être faits des renseignements personnels concernés et les personnes à qui ceux-ci peuvent être communiqués. Le Commissariat a aussi recommandé que Transports Canada lance une campagne de sensibilisation du public transparente et détaillée par le biais des grands médias afin de décrire les pratiques en matière de renseignements personnels dans le contexte du PPP, y compris les mécanismes de recours.

Possibilité de porter plainte à l'égard du non-respect des principes — L'EFVP mentionne que Transports Canada ne dispose d'aucune procédure précise concernant l'enregistrement, le traitement et la résolution des plaintes. Le Commissariat a recommandé d'établir et de documenter des procédures de fonctionnement normalisées à l'intention du Bureau de réexamen avant la mise en œuvre du PPP.

État actuel

- En 2009, le Commissariat a présenté au Parlement un rapport de vérification qui examinait si Transports Canada avait en place des mesures de contrôle et de sécurité visant la collecte, l'utilisation, la communication, la conservation, le retrait, la protection et l'exactitude des renseignements personnels dans le cadre du PPP.
- La vérification a permis de conclure que dans le cadre du PPP, Transports Canada recueille et utilise des renseignements personnels dans le respect de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'aéronautique*, mais aussi que le sous-ministre de Transports Canada ne disposait pas de renseignements complets au moment d'ajouter ou de soustraire des noms à la LPP.
- La situation pourrait soulever des préoccupations quant au processus décisionnel si un dossier incomplet devait entraîner une modification erronée à la LPP.
- En outre, Transports Canada n'a pas pu démontrer que le système informatique servant à communiquer les renseignements compris dans la LPP aux transporteurs aériens avait été certifié conforme aux normes de sécurité du gouvernement.
- Transports Canada a accepté toutes les recommandations formulées au terme de la vérification et a entrepris de les mettre en œuvre. Le Commissariat fera un suivi après deux ans.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Étude de cas n^{o} 2 : scanners à ondes millimétriques dans les aéroports de l'Administration canadienne de la sûreté du transport aérien

L'Administration canadienne de la sûreté du transport aérien (ACSTA) est une société d'État chargée de protéger le public en effectuant une vérification pré-embarquement des voyageurs aériens et de leurs bagages ainsi que des non-voyageurs qui ont accès à des zones d'accès restreint. En août 2009, l'ACSTA a présenté une évaluation des facteurs relatifs à la vie privée (EFVP) au Commissariat sur le déploiement des scanners à ondes millimétriques (OMM) dans les aéroports canadiens. Cette technologie passe à travers les vêtements des voyageurs et montre des images du corps afin de détecter des armes et des explosifs qui ne pourraient être détectés autrement.

Son utilisation est controversée et fait l'objet de grandes inquiétudes tant au Canada qu'à l'étranger. Selon l'ACSTA, cependant, la technologie à OMM constitue une approche novatrice pour inspecter les passagers puisqu'elle est moins envahissante que la fouille manuelle utilisée actuellement dans les aéroports canadiens. Les passagers qui subissent un deuxième contrôle pourraient choisir entre la fouille manuelle ou la technologie à OMM. En outre, selon l'ACSTA, cette technologie constitue une amélioration par rapport aux systèmes de détection des menaces actuels comme les détecteurs de métal, car elle permet de trouver des armes qui ne sont pas en métal.

L'ACSTA est consciente que les scanners à OMM soulèvent des préoccupations en matière de protection de la vie privée. Elle dit avoir pris un certain nombre de mesures pour répondre à ces préoccupations et ainsi améliorer la protection de la vie privée, y compris : faire en sorte que le processus de contrôle à OMM soit volontaire et anonyme; ne faire aucun lien entre une image obtenue à l'aide d'une OMM et le nom du passager ou tout autre renseignement permettant de l'identifier; veiller à ce que les images prises par le système à ondes durant le contrôle ne puissent pas être vues ou transmises à un autre endroit; permettre seulement à des opérateurs qualifiés et autorisés d'utiliser le système; faire en sorte que les imageurs à OMM ne puissent enregistrer, imprimer ou sauvegarder des images.

Critère en quatre parties : nécessité, efficacité, proportionnalité et autres solutions possibles

L'ACSTA a assuré au Commissariat que la nécessité de la technologie à OMM repose sur une évaluation rigoureuse des menaces et des risques en matière de sécurité aérienne. Le Commissariat soutient néanmoins que l'ACSTA devrait examiner régulièrement la mise en œuvre de la technologie à OMM et la justifier en fonction du critère en quatre parties. Le Commissariat a recommandé à l'ACSTA d'examiner régulièrement la nécessité perçue de cette technologie par rapport à de nouvelles évaluations des menaces et des risques pour la sécurité aérienne et au perfectionnement des technologies disponibles. Il recommande surtout d'envisager des technologies nouvelles ou de remplacement qui permettent d'atteindre les mêmes objectifs de contrôle tout en portant moins atteinte à la vie privée. L'ACSTA a rétorqué que les logiciels disponibles pour brouiller les images de certaines parties du corps iraient à l'encontre de l'objectif de la technique.

L'ACSTA a aussi informé le Commissariat qu'elle ferait l'essai de logiciels améliorés pour les unités à OMM qui permettraient aux scanners de relever les anomalies sans générer des images réelles des voyageurs. Les responsables de la sécurité verraient seulement un bonhomme-allumettes dont certaines parties du corps seraient mises en évidence pour effectuer une fouille corporelle ciblée. Si le projet pilote est une réussite, le plan consisterait à déployer le nouveau logiciel dans tous les scanners à OMM des aéroports canadiens. Cette mesure est conforme à la recommandation du Commissariat qui consiste à étudier de façon approfondie de nouvelles technologies pour améliorer la protection de la vie privée.

Principes relatifs à l'équité dans le traitement de l'information

Responsabilité — L'ACSTA a mentionné être déterminée à mener des vérifications sur le respect des politiques en matière de protection de la vie privée.

Détermination des fins de la collecte des renseignements — L'ACSTA a indiqué que des avis précisant les fins de la collecte des renseignements au moyen de la technologie à OMM seraient diffusés aux points de contrôle de sûreté des aéroports équipés de scanners. Le Commissariat recommande aussi que l'ACSTA mène une campagne de sensibilisation du public sur son site Web, dans les aéroports à l'aide d'affiches et de brochures et en utilisant d'autres sources d'information.

Consentement et avis — L'ACSTA a mentionné que les voyageurs choisis pour subir un deuxième contrôle pourraient choisir entre la technologie à OMM et une fouille manuelle. Le Commissariat a aussi recommandé que le matériel de communication de l'ACSTA reproduise précisément les images obtenues au cours du contrôle pour garantir un consentement éclairé. Enfin, le Commissariat a recommandé à l'ACSTA d'examiner attentivement des questions précises en ce qui a trait à l'utilisation de la technologie à OMM pour contrôler les mineurs et les personnes aux prises avec des difficultés physiques.

Limitation de la collecte — Le Commissariat a recommandé que le scanner recueille seulement l'image transitoire.

Limitation de l'utilisation, de la communication et de la conservation — L'ACSTA devrait préciser la durée pendant laquelle les images transitoires existeront.

Exactitude — Selon l'EFVP, les images produites par les scanners à OMM sont celles de la personne qui se trouve dans l'unité de contrôle. Toute anomalie serait examinée et confirmée par un agent au point de contrôle, au moyen d'observations ou d'une fouille manuelle ciblée.

Mesures de sécurité — Selon l'EFVP, les images produites seront supprimées définitivement une fois le contrôle terminé et elles seront envoyées par voie électronique à la salle de télésurveillance, de sorte que l'agent de contrôle des images ne puisse voir et identifier le voyageur. Le Commissariat a aussi recommandé que l'ACSTA entreprenne des évaluations pour assurer la sécurité des images électroniques et en empêcher l'utilisation ou la communication inappropriées.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Transparence — Le Commissariat a recommandé à l'ACSTA d'élaborer et de rendre publique une politique sur le respect de la vie privée se rapportant précisément à l'utilisation des scanners à OMM.

Accès aux renseignements personnels — L'ACSTA a fait remarquer que les personnes ne pourront avoir accès à leurs images, car celles-ci ne seront pas enregistrées et seront impossibles à identifier individuellement lorsque les responsables de la sécurité les visionneront.

Possibilité de porter plainte à l'égard du non-respect des principes — Au moment de la rédaction de l'EFVP, il n'y avait aucune procédure de respect de la vie privée permettant aux voyageurs de déposer une plainte auprès de l'ACSTA. Le Commissariat a recommandé que l'ACSTA surveille les commentaires, les plaintes et les préoccupations qu'elle reçoit des voyageurs et qu'elle en fasse rapport à la haute direction.

État actuel

- L'ACTSA a accepté la recommandation du Commissariat voulant que les scanners ne soient utilisés que pour l'étape de contrôle secondaire.
- L'ACTSA s'est également engagée à ce que :
    - la participation demeure anonyme et volontaire;
    - une fouille par palpation soit offerte comme mesure de rechange;
    - les agents de contrôle soient situés dans un endroit isolé d'où ils ne peuvent pas voir la personne soumise au scanner;
    - les images ne soient associées à aucun autre renseignement personnel et ne puissent pas être identifiées;
    - toutes les images soient supprimées immédiatement après la fin du balayage.
- Le Commissariat continue de suivre les activités de l'ACTSA et encourage l'Agence à rester à l'affût de nouvelles technologies qui permettraient de restreindre davantage le caractère envahissant des mesures de sécurité dans les aéroports.
- L'ACTSA effectue présentement l'examen d'un logiciel qui n'a pas besoin de générer une image du corps. Un logiciel qui produit une image qui ressemble davantage à un schéma qu'à une image naturelle du corps humain fait également l'objet d'un projet pilote.
- Le Commissariat a entamé une vérification des mesures de sécurité du transport aérien, afin d'examiner les pratiques de gestion des renseignements personnels et les technologies de contrôle de la sécurité. Cette vérification devrait être terminée l'an prochain.

Étude de cas n^{o} 3 : Permis de conduire Plus de l'Agence des services frontaliers du Canada

À la suite des enquêtes sur les attentats du 11 septembre 2001 à New York et à Washington D.C., le gouvernement des États-Unis a commencé à mettre en œuvre une série de nouveaux programmes, lois et mesures en matière de sécurité, dont l'Initiative relative aux voyages dans l'hémisphère occidental (IVHO). Celle-ci impose de nouvelles exigences concernant les documents d'identité sûrs que doivent transporter les personnes qui se rendent aux États-Unis par voie aérienne, terrestre ou maritime. Les citoyens canadiens n'ont pas été exemptés des exigences de l'IVHO élaborée par le département de la Sécurité intérieure (DSI) des États-Unis.

Les responsables canadiens craignaient l'incidence négative que les nouvelles exigences de l'IVHO pourraient avoir sur le commerce et les voyageurs. Les passeports ou d'autres documents sûrs étant nécessaires pour franchir la frontière vers les États-Unis à partir de juin 2009, le Canada et les États-Unis ont immédiatement consacré des efforts pour élaborer des documents sûrs de remplacement, dont le permis de conduire Plus (PC Plus). L'Agence des services frontaliers du Canada était le ministère fédéral responsable au Canada.

L'ASFC est l'organisme fédéral chargé de voir à la sécurité du pays en gérant l'accès des personnes et des marchandises qui entrent au Canada ou qui en sortent. Elle a entrepris un projet pour favoriser l'adoption de plans relatifs aux PC Plus dans les provinces canadiennes et assure le lien avec le Service des douanes et de la protection des frontières des États-Unis (SDPF). L'ASFC gère aussi la base de données des PC Plus à laquelle les États-Unis ont accès.

Le plan concernant le PC Plus (Étape I, projet pilote en Colombie-Britannique, 2007)

En mars 2007, le gouvernement de l'État de Washington a commencé à élaborer un PC Plus pour respecter les exigences émises par le DSI. Compte tenu du volume de la circulation des biens et des gens à la frontière, les responsables de l'État de Washington ont communiqué avec le gouvernement de la Colombie-Britannique pour évaluer leur intérêt à participer à un projet pilote. Les responsables fédéraux des deux pays se sont aussi réunis pour discuter des répercussions des nouvelles exigences relatives aux pièces d'identité sur les périodes d'attente aux frontières. Les autorités provinciales de l'Ontario et du Québec ont aussi manifesté leur intérêt à participer.

À la suite de ces discussions, il a été décidé que les gouvernements provinciaux du Canada créeraient les PC Plus et que les données sur les détenteurs de PC Plus du Canada seraient ensuite réunies par l'ASFC et transmises au SDPF. En plus des données traditionnellement contenues dans les permis de conduire, chaque PC Plus comprendrait un indicateur de citoyenneté, une puce d'identification par radiofréquence et un numéro d'identification unique pour que les autorités frontalières américaines puissent consulter instantanément le dossier d'un détenteur de PC Plus avant qu'il arrive au poste frontalier, ce qui accélérerait le contrôle et le traitement.

Les demandeurs du PC Plus consentiraient à ce que tous ces renseignements soient échangés avec l'ASFC et le DSI au moment où ils présentent leur demande. Ils

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

autoriseraient aussi l'échange de renseignements personnels entre les autorités frontalières, les autorités de l'immigration, les organismes d'application de la loi et d'autres organismes gouvernementaux, tant au Canada qu'aux États-Unis. Par exemple, une vérification des antécédents serait effectuée pour confirmer le statut de citoyen. L'échange de renseignements avec le SDPF et le DSI vise à permettre d'effectuer des contrôles en fonction des listes de surveillance contre le terrorisme et d'appliquer d'autres moyens de surveillance à la frontière américaine.

L'échange de renseignements sur les participants canadiens ne serait cependant pas réciproque. L'ASFC ne prévoit pas recueillir à l'avance des données supplémentaires sur les citoyens américains qui voyagent au Canada. Au début de 2007, les responsables de la protection de la vie privée aux niveaux provincial et fédéral ont commencé à manifester leurs inquiétudes concernant le projet de PC Plus de l'ASFC. Le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a aussi soulevé une vaste gamme de préoccupations. À la fin de 2007, l'ASFC a invité les responsables de la protection de la vie privée à aborder ces questions directement avec le DSI et le département d'État des États-Unis pour plus de clarté.

Critère en quatre parties : nécessité, efficacité, proportionnalité et autres solutions possibles

Plusieurs risques liés à la protection de la vie privée ont immédiatement été mis de l'avant lors des échanges entre le Commissariat et l'ASFC : l'utilisation de puces d'identification par radiofréquence de longue portée dans les PC PLUS pouvant être lues à distance, la création par l'ASFC d'une « base de données miroir » sur les détenteurs de PC Plus de chaque province, le transfert par l'ASFC d'une grande quantité de renseignements personnels sur les détenteurs de PC Plus au DSI et l'ajout d'éléments indiquant la citoyenneté et l'identité dans un simple permis. Certains changements étaient nécessaires (étant donné que les changements provoqués par l'IVHO sont essentiellement imposés par les États-Unis, qui ont un pouvoir souverain sur leurs propres frontières), mais les arguments pour étayer la nécessité du PC PLUS étaient faibles. Les passeports canadiens permettent encore d'atteindre les objectifs et ils sont toujours requis pour se rendre aux États-Unis par avion.

Le Commissariat soutenait qu'aucun motif clair n'explique pourquoi il serait impossible qu'un serveur de l'ASFC au Canada héberge les renseignements du PC PLUS, que le SDPF pourrait interroger au besoin. L'ensemble des preuves présentées sur l'efficacité du Programme était loin d'être convaincant : aucune analyse claire n'a été présentée pour montrer l'incidence des PC PLUS sur les périodes d'attente. Cette ambigüité a grandement compliqué la discussion sur la proportionnalité de la proposition.

En fin de compte, le Commissariat a insisté sur le besoin de réexaminer sérieusement les questions suivantes : a) l'exportation de données en bloc; b) la sensibilisation du public et le consentement pleinement éclairé des demandeurs; c) l'utilisation sécuritaire d'une technologie d'identification par radiofréquence non cryptée à faible distance; d) la collecte de renseignements strictement nécessaires pour gérer le Programme seulement; e) l'examen et la surveillance efficaces du Programme.

Principes relatifs à l'équité dans le traitement de l'information

Responsabilité — L'ASFC a accordé beaucoup d'importance à sa responsabilité concernant l'entretien et la garde des données. En 2009, elle est revenue sur sa décision d'enregistrer de grandes quantités de données sur des CD pour les transférer aux États-Unis. Elle a plutôt décidé de créer un serveur pour administrer les PC Plus. Les autorités frontalières des États-Unis pourront l'interroger lorsqu'on leur présentera un PC Plus canadien. En outre, en 2010, l'ASFC s'est engagée à nommer son propre responsable de la protection de la vie privée pour superviser des programmes comme le PC Plus.

Détermination des fins de la collecte des renseignements — L'ASFC a collaboré avec le Commissariat et les autorités provinciales responsables de la protection de la vie privée pour rédiger dans un langage clair et précis les fins auxquelles divers renseignements personnels étaient recueillis.

Consentement et avis — La participation au Programme était entièrement volontaire. Les demandeurs ont reçu des renseignements détaillés sur le Programme; ces renseignements étaient répétés et expliqués au cours de l'entrevue et du processus d'inscription. Le fait que des renseignements personnels seraient communiqués à des autorités américaines en application des lois américaines était répété tout au long du processus.

Limitation de la collecte — L'ASFC a réaffirmé qu'aucun renseignement personnel ne serait enregistré sur les puces à identification par radiofréquence ou recueilli pour alimenter les bases de données nécessaires pour les PC Plus.

Limitation de l'utilisation, de la communication et de la conservation — L'ASFC a affirmé que le PC Plus servirait seulement à établir l'identité, la citoyenneté et l'admissibilité des voyageurs qui veulent entrer aux États-Unis. Des protocoles d'entente ont été élaborés pour établir ces contrôles.

Exactitude — Le Commissariat était d'abord préoccupé par la question d'assurer l'exactitude des modifications apportées aux données des PC Plus qui seront transférées aux États-Unis. La décision prise par l'ASFC de maintenir les données au Canada, et ainsi de permettre l'accès aux renseignements personnels et la correction de ceux-ci, est une amélioration.

Mesures de sécurité — Tous les employés qui traitent les renseignements personnels sur les PC Plus détiendraient une cote de sécurité de niveau secret, qui est obtenue après un examen du casier judiciaire par la GRC et une vérification des antécédents par le SCRS. Des mesures strictes ont été mises en place pour contrôler l'accès aux données aux niveaux provincial et fédéral. Une pochette protectrice contre l'« écrémage » des permis PC Plus a été produite pour empêcher la lecture à distance.

Transparence — L'ASFC s'est engagée à aborder expressément la question de l'accès du gouvernement américain aux données dans ses communications avec le public canadien pour veiller à ce que celui-ci connaisse les importantes mesures de protection de la vie privée qui seront mises en place, surtout en ce qui a trait aux échanges avec les États-Unis dans le contexte de la *USA PATRIOT Act*.

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Accès aux renseignements personnels — Conformément aux termes de la *Loi sur la protection des renseignements personnels* et les actes législatifs provinciaux pertinents.

État actuel

- À l'été 2009, l'ASFC a publié sur son site Web un résumé détaillé du processus d'EFVP lié au programme de PC Plus, y compris des précisions sur la manière dont les détenteurs de PC Plus peuvent accéder à leurs renseignements personnels.
- En date de 2010, les PC Plus sont offerts en Colombie-Britannique, en Ontario, au Québec et au Manitoba.

Annexe B : Politique, directives et documents d'orientation du Conseil du Trésor relatifs à la protection de la vie privée

- Politique sur la protection de la vie privée
- Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché
- Document d'orientation pour aider à préparer des ententes d'échange de renseignements personnels
- Directive sur le numéro d'assurance sociale
- Directive concernant l'administration de la *Loi sur l'accès à l'information*
- Directive sur les demandes de renseignements personnels et de correction
- Directives sur les pratiques relatives à la protection de la vie privée
- Directive sur l'évaluation des facteurs relatifs à la vie privée
- Lignes directrices — Généralités — 2-00
- Rôles et responsabilités — Protection des renseignements personnels et des données — 2-01
- Collecte de renseignements personnels — 2-02
- Conservation et retrait des renseignements personnels — 2-03
- Usage et communication de renseignements personnels — 2-04
- Droit d'accès aux renseignements personnels — 2-06
- Corrections et mentions des corrections — 2-07
- Renseignements exclus — 2-08
- Exceptions — Protection des renseignements personnels et des données — 2-09
- Examen des décisions prises en vertu de la *Loi sur la protection des renseignements personnels* — 2-10
- Rapports annuels — Protection des renseignements personnels et des données — 2-11
- Délégation d'autorité — 3-01
- Aide aux personnes dans l'exercice de leurs droits — 3-02
- Code de la protection des renseignements personnels concernant les employés — 3-03
- Formulaires — Protection des renseignements personnels et des données — 3-05
- Lettres types — Protection des renseignements personnels et des données — 3-06

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190

Annexe C : Autres ressources, références et documents utiles

- Centre for Innovation Law and Policy. Personal Information Protection in the Face of Crime and Terror: Information Sharing by Private Enterprises for National Security and Law Enforcement Purposes, (Université d'Ottawa, 2008)
- Chambre des lords, Select Committee on the Constitution (R.-U.). *Surveillance: Citizens and the State* (février 2009)
- Cockfield, Arthur J. « Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies », *U.B.C. Law Review*, vol. 40, n° 1 (mai 2007), p. 41
- Cohen, Stanley. *Privacy, Crime and Terror — Legal Rights and Security in a Time of Peril* (Butterworths, 2005)
- Commissariat à l'information et à la protection de la vie privée de l'Ontario. *Privacy Risk Management* (2010)
- Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India. Vol 182 d'Air India : Une tragédie canadienne – Rapport final (2010)
- Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (1979-1981)
- Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar. Analyse et recommandations (2006)
- Ibid. Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale (2006)
- Commission internationale de juristes (CIJ), panel de juristes sur le terrorisme, la lutte contre le terrorisme et les droits de la personne. *Assessing Damage, Urging Action* (2009)
- Forcese, Craig. *The Collateral Casualties of Collaboration: The Consequence for Civil and Human Rights of Transnational Intelligence Sharing* (mars 2009)
- Gouvernement du Canada. *Protéger une société ouverte : la politique canadienne de sécurité nationale* (avril 2004)
- Harvey, Frank. *The Homeland Security Dilemma: Imagination, Failure and the Escalating Costs of Perfecting Security* (2007)
- Posner, Richard A. « Orwell versus Huxley: Economics, Technology, Privacy, and Satire », Faculté de droit de l'Université de Chicago, John M. Olin Law & Economics *Working Paper* n° 89 (novembre 1999)
- Regan, Priscilla M. *Legislating Privacy: technology, social values and public policy* (UNC Press, 1995)
- Schienin, Martin. *The Right to Privacy: Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism* (Conseil des droits de l'homme des Nations Unies, décembre 2009)
- Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer, 2006)
- Soghoian, Christopher. « Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era », *Journal of Telecommunications and High Technology Law*, Forthcoming; Berkman Center Research, publication n° 2009-07 (17 août 2009)
- Solove, Daniel J. « A Brief History of Information Privacy Law », Faculté de droit de l'Université George Washington, *Public Law Research Paper* n° 215

- Solove, Daniel J. « Digital Dossiers and the Dissipation of Fourth Amendment Privacy », *Southern California Law Review*, vol. 75, juillet 2002
- Solove, Daniel J. « 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy », *San Diego Law Review*, vol. 44, 2007
- W. Diffie et S. Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 2007)
- Wright, Andrea. « Casting a light into the shadows: why security intelligence requires democratic control, oversight and review », *The Human Rights of Anti-Terrorism* (Irwin Law, 2008), p. 327-367

priv.gc.ca | San frais : 1-800-282-1376 | Téléphone : (613) 947-1698
Téléc. : 613-947-6850 | ATS : (613) 992-9190