Cahier de recherche

Flux transfrontières de données et protection de la vie privée : une conjonction difficile

Monica Tremblay, M.Sc.
Anthropologue

Laboratoire d'étude sur les politiques publiques et la mondialisation

École nationale d'administration publique

Vol. III, n°1, mars 2010

Laboratoire d'étude
sur les politiques publiques
et la mondialisation

Flux transfrontières de données et protection de la vie privée : une conjonction difficile

MONICA TREMBLAY, M.Sc.

La libéralisation des échanges et la diffusion des technologies de l'information accentuent les flux transfrontières de données. Les renseignements personnels peuvent être entreposés dans un ou plusieurs pays, ce qui soulève des inquiétudes quant à leur protection et au respect de la vie privée. À quel point la vie privée des personnes qui ont fourni des renseignements personnels sous un système législatif particulier peut-elle être protégée à l'étranger ? Il semble que les lois actuelles accusent un retard certain par rapport aux flux de données et ne permettent pas d'en assurer la protection en cas de transfert à l'étranger. Ce texte examine la portée des lois censées protéger la vie privée. Il donne un aperçu de la situation légale en matière de protection des renseignements personnels dans des pays directement concernés par les flux de données. Il fait ressortir le besoin d'une protection internationale de ces renseignements et de la vie privée, protection qui devra être soutenue par la recherche et la coopération internationale.

Vol. III, n°1, mars 2010

Introduction

Différents mécanismes de la mondialisation accentuent le flux des données à caractère personnel entre les pays. Avec l'évolution des nouvelles technologies de l'information et des communications (NTIC) et la libéralisation des échanges, l'impartition de programmes et services vers des pays étrangers est en augmentation dans les secteurs privé et public. Dès lors, les entreprises peuvent plus facilement disposer d'antennes dans différents pays. Le phénomène est bien connu à cause de la délocalisation de centres d'appels ou de traitement de l'information. Le fonctionnement des sites de réseautage social ou d'applications commerciales en ligne illustre également cette tendance à recourir à des tierces parties en divers endroits de la planète afin d'offrir un service de portée mondiale[1]. Les renseignements personnels[2] peuvent ainsi se trouver entreposés dans un ou plusieurs pays. Cette façon de faire est très intéressante puisqu'elle comporte divers avantages, particulièrement d'ordre économique et de gestion de l'information. Elle soulève par contre des inquiétudes concernant la protection des renseignements personnels et de la vie privée, en plus de problèmes liés à la sécurité informatique, à la perte ou au vol des renseignements.

Lorsque des renseignements personnels sont transférés à l'étranger, qu'advient-il de leur protection et du respect de la vie privée ? Quelle est la portée des lois censées protéger la vie privée lorsque des données à caractère personnel sortent du pays où elles ont été collectées ? Il semble que les lois actuelles accusent un retard par rapport aux flux des données et ne permettent pas d'en assurer la protection en cas de transfert à l'étranger. Certes, ces lois peuvent orienter le choix de transférer, ou non, les données vers l'étranger, dans un pays plutôt qu'un autre, ou guider l'adoption de mesures particulières, selon le cas. Cependant, les lois du pays d'origine ne parviennent pas à assurer la même protection lorsque les données sortent de son territoire.

Dans ce texte, il sera question de la gestion des données lorsqu'elles sont transférées dans un autre pays. À quel point la vie privée des personnes qui ont fourni des renseignements personnels sous un système législatif particulier peut-elle être protégée à l'étranger ? Il semble pertinent de se demander si les lois actuelles visant à protéger les renseignements personnels sont efficaces en cas de flux transfrontières de données[3]. Cette question se pose avec acuité dans le contexte de la lutte contre le terrorisme international qui entraîne, à des fins de sécurité nationale, la mise en place

[1] Cela fait appel à l'utilisation de ce que l'on désigne par le terme de « cloud computing » traduit par « informatique dans les nuages ». Il s'agit d'une approche technique permettant de délocaliser géographiquement le traitement et l'entreposage de l'information.

[2] Toutes les données qui permettent d'identifier une personne - équivalent du terme « données nominatives » utilisé en Europe.

[3] « Flux de données transfrontières » signifie le transfert de données, pouvant être des renseignements personnels ou des renseignements de nature délicate, vers l'étranger (SCT, 2006:1).

de mesures qui pourraient avoir un impact sur la vie privée. Comment s'accordent les États entre eux à cet égard ?

La première partie de ce texte esquisse le problème et emprunte aux recherches à ce sujet. La deuxième partie pose un regard sur les directives de l'OCDE (Organisation de coopération et de développement économiques) et sur les lois de l'Union européenne, du Canada, du Québec et des États-Unis en matière de protection des données à caractère personnel dans le cas de transfert vers un autre pays. Elle donne aussi un aperçu de la situation légale de la protection des renseignements personnels dans des pays de grande impartition, tels que l'Inde. La dernière partie fait ressortir le besoin d'une protection internationale des renseignements et de la vie privée dans un contexte favorable aux flux transfrontières de données.

1. Contexte actuel

Dans tous les États, des organisations publiques et privées recueillent et détiennent à différentes fins des renseignements à caractère personnel. Au-delà de la mission qu'elles poursuivent et des services qu'elles offrent, les organisations tentent généralement d'être plus efficaces dans la gestion de ces données, principalement afin de réduire les coûts de traitement. Elles se préoccupent aussi d'assurer la sécurité des données qu'elles détiennent. Chacune s'engage à sa façon, selon les lois et politiques en vigueur, à protéger les renseignements et la vie privée des personnes qui ont fourni cette information (Martin et Rabina, 2009).

Dans leur quête d'efficience, certaines organisations s'engagent sur la voie du transfert de données à l'étranger (Martin et Rabina, 2009; Holder et Grimes, 2007; Karyda, Mitrou et Quirchmayr, 2006). Elles tirent ainsi profit de l'expertise disponible en plusieurs lieux sur la planète. L'organisation qui possède un bureau dans un autre pays peut y transférer ses données. Elle peut aussi décider de déléguer à une entreprise à l'étranger quelques-unes de ses tâches, telles que l'hébergement et le traitement des données, ou encore confier des renseignements à une entreprise étrangère installée dans le même pays. Dans cette situation, il est alors possible que l'entreprise étrangère effectue le travail qui lui est demandé dans un autre pays, peut-être à son siège social où à un autre endroit qui lui permet d'offrir le même travail à moindre coût. Les centres d'appels installés en Inde, qui desservent des entreprises canadiennes, en sont un exemple. Grâce à Internet, les données demeurent facilement accessibles, comme si elles étaient au pays.

Le flux transfrontière de données s'observe notamment dans les services financiers ainsi que dans les domaines de l'éducation, des ressources humaines, du commerce électronique et de la santé (OCDE, 2006; Holder et Grimes, 2007). Les banques de données de certaines institutions financières canadiennes peuvent être hébergées aux États-Unis. L'exemple de la banque CIBC, qui avait imparti des services à un fournisseur situé aux États-Unis, a d'ailleurs soulevé de réelles craintes. Cette façon de procéder augmentait les risques de porter atteinte à la vie privée des personnes en permettant aux autorités américaines l'accès à tous les renseignements ainsi hébergés, sans l'autorisation des clients. Par la suite, en 2004, la Colombie-Britannique a interdit aux organismes publics de communiquer et de stocker des renseignements personnels à l'étranger. Des bases de données canadiennes contenant des renseignements personnels ont même été rapatriées. Pour sa part, en 2006, le Commissaire à la protection de la vie privée de l'Alberta ne recommandait pas d'interdire ce type de transfert mais plutôt de définir des politiques et des « solutions légales contractuelles et opérationnelles plus souples » (Kosseim, 2006:3).

Vers la fin des années 1990, des chercheurs ont commencé à se préoccuper du recours aux services du secteur privé par le secteur public. Ils craignaient notamment que les organisations gouvernementales qui ont recours à l'impartition perdent le contrôle de

leurs données, de leurs décisions et du service dont elles ont la responsabilité (Martin et Rabina, 2009).

Le haut degré de sophistication des technologies de l'information, des communications et de surveillance exacerbe aussi les inquiétudes, car elles permettent désormais une diversité exponentielle de traitement de l'information. On peut les utiliser, par exemple, afin d'extraire des renseignements intégrés dans une banque de données (*data mining* — forage de données) ou encore de croiser des informations qui serviront au profilage dans la poursuite d'un objectif de lutte contre le terrorisme (Leonard et Mention, 2008; Gunasekara, 2007).

Les préoccupations se sont étendues et ont touché tous les types d'organisations. On s'est alors demandé ce qu'il advient de la protection de la vie privée des personnes lorsqu'un gouvernement, au nom de la sécurité nationale et internationale, recueille des données à caractère personnel dans le but d'exercer une meilleure surveillance contre le terrorisme[4]. Nombreux sont les pays qui ont édicté des lois antiterroristes et des mesures de sécurité qui confèrent à certaines instances gouvernementales des droits particuliers d'accès aux données détenues sur leur territoire par des entreprises et organisations. La plus connue de ces lois est sans doute le USA PATRIOT Act[5], en vertu duquel une entité gouvernementale peut exiger d'obtenir et de consulter les informations dont dispose toute organisation basée sur le territoire des États-Unis (USA PATRIOT Act, article 215).

Les questions concernant l'équilibre entre sécurité et vie privée ont dès lors été soulevées par des experts (Chandler, 2009; Gunasekara, 2007; Stefanick, 2007). Chandler soutient qu'il faudrait vérifier si l'obtention de données personnelles augmente la sécurité et si le même résultat pourrait être atteint autrement. À l'aide d'exemples de renseignements personnels recueillis à des fins de sécurité, Stefanick avance que la frontière entre la quête de sécurité et l'augmentation des risques d'atteinte à la vie privée reste à définir.

Certains spécialistes se sont intéressés aux mesures de contrôle, de type plus technique, visant à minimiser les risques d'atteinte à la protection des renseignements personnels et de la vie privée en cas d'impartition. Certes, ils conviennent de la nécessité d'établir des ententes entre les organisations engagées dans de telles opérations. Ces ententes permettent, par exemple, de bien définir l'objet de la collecte d'informations et de s'assurer de la surveillance des accès aux registres. Ces

[4] À la suite d'une consultation publique, le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a proposé « que les mesures existantes de protection des renseignements personnels fassent l'objet d'un examen de la part de toutes les administrations à l'échelle du Canada et au niveau international, et ce, tant dans les secteurs public que privé », suggestion qu'a approuvée la Commissaire à la protection de la vie privée du Canada (SCT, 2006:11).

[5] « USA PATRIOT » acronyme de « Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ».

précautions semblent toutefois insuffisantes pour protéger adéquatement la vie privée (McDonagh *in* Martin et Rabina, 2009; Ovenden, 2009; Haden, 2006).

Le principal problème soulevé par plusieurs chercheurs et spécialistes en matière de protection des renseignements personnels et de la vie privée, lorsque des données traversent des frontières, résulte du changement de législation qui rendrait plus vulnérables certaines dimensions de la vie privée (Martin et Rabina, 2009; Stefanick, 2007; Poullet, 2007; Gunasekara, 2007; Caruana et Cannataci, 2007; Leonard et Mention, 2008). Les données à caractère personnel détenues par les organisations sont protégées de différentes façons selon les pays, particulièrement en fonction de l'existence ou non de lois destinées à protéger de tels renseignements et la vie privée (Martin et Rabina, 2009; Comeau, 2002; Gunasekara, 2007; Holder et Grimes, 2007). Dès que les renseignements migrent vers un autre territoire, la protection à laquelle pourraient s'attendre les personnes qui les ont confiés peut être affectée. Si une organisation installée dans un pays tiers et détenant des renseignements personnels fait un mauvais usage de ces données, aucun recours légal ne semble disponible (McGullagh, 2009; Fuster, De Hert et Gutwirth, 2008). Les citoyens n'ont alors aucun moyen de défendre leurs droits (Stefanick, 2007).

Diverses démarches visant à réglementer le flux des données ont été relevées dans différents pays (Gunasekara, 2007). Actuellement, les lois de protection de la vie privée ont valeur dans un État précis et ne couvrent pas les renseignements personnels lorsqu'ils sortent du pays qui les a recueillis; c'est notamment le cas de la Directive de 1995[6] de l'Union européenne, de la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDÉ) du Canada et des lois québécoises de protection des renseignements personnels dans les secteurs public et privé. C'est la loi du pays où se trouvent les données qui s'applique en cas de nécessité (CPVP, 2008; Poullet, 2007; Léonard et Mention, 2008; Martin et Rabina, 2009). Gunasekara (2007) fait remarquer que dans le contexte de la mondialisation, où les biens et services se déploient au-delà des frontières, les différentes mesures de protection de la vie privée de chaque État sont plutôt faibles, étant donné qu'en un « clic » de souris, l'information peut être déplacée et régie sous un autre système légal.

Plusieurs relèvent la nécessité d'une protection des renseignements personnels et de la vie privée à l'échelle mondiale et signalent le besoin d'efforts conjoints afin d'atteindre un tel résultat (Kosseim, 2006; SCT, 2006; Holder et Grimes, 2007; Poullet, 2007; Gunasekara, 2007). Selon Holder et Grimes, l'élaboration de lois visant à protéger les renseignements personnels n'a pas fait l'objet d'une concertation à l'échelle mondiale. On déplore même l'absence de cohérence entre les pays qui affichent un certain leadership en la matière. Selon d'autres auteurs, les principes de base de la protection

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

des renseignements personnels sont mal définis (McCullagh, 2009) ou tiennent compte de la seule réalité culturelle du pays où s'applique la loi (Poullet, 2007).

Certains auteurs mentionnent le besoin de développer de nouveaux protocoles de respect de la vie privée ou de revoir les lois de protection des renseignements personnels à la lumière des nouvelles exigences qu'imposent les flux de données transfrontières. L'objectif est de trouver un équilibre entre flux, accès aux renseignements et protection de la vie privée (Gunasekara, 2007; Poullet, 2007; Martin et Rabina, 2009; McCullagh, 2009; Léonard et Mention, 2008; Karyda, Mitrou et Quirchmayr, 2006; SCT, 2006). Selon Gunasekara et Poullet notamment, les approches actuelles visant à réglementer les flux de données transnationaux sont déficientes au regard de la protection de la vie privée. Il y a un besoin de dispositions à portée extraterritoriale (Poullet, 2007). Les Commissaires à la protection des données et à la vie privée, des groupes de pression et les chefs d'État et de gouvernement de la Francophonie revendiquent aussi, depuis quelques années déjà, l'élaboration de normes internationales. Ils invoquent le besoin « d'un instrument juridique universel contraignant » (Conférence internationale des Commissaires à la protection des données, 2009; Sommet de la Francophonie, 2006). Assurer la protection des renseignements personnels qui traversent les frontières représente un chantier en friche (Martin et Rabina, 2009).

Outre les différences entre les lois, d'un pays à l'autre, certains auteurs ont observé des nuances dans la conception et l'interprétation des notions telles que « renseignements personnels » et « vie privée ». Cette observation a été relevée même entre pays occidentaux qui ont des référents culturels similaires. McCullagh (2009) a remarqué que l'interprétation par le Royaume-Uni du concept de « données personnelles » diffère de ce qui sous-tend la Directive de 1995 de l'Union européenne.

D'autres se sont penchés sur l'influence de la culture quant à l'importance accordée à certaines notions (Holder et Grimes, 2007; Poullet, 2007). Caruana et Cannataci (2007) rappellent que la vie privée n'est pas un droit humain universellement reconnu. Ainsi, Hayat (2007), auteur du projet de loi sur la protection des données au Pakistan, considère la vie privée suffisamment protégée par la Constitution pakistanaise, laquelle est structurée autour des principes de la religion islamique. Cela s'avère insatisfaisant aux yeux de la Commission européenne.

2. Mesures nationales et internationales

Depuis les années 1970 et 1980, beaucoup de pays ont adopté des lois en matière de protection de la vie privée et des renseignements personnels. Presque tous les États de l'OCDE disposent de telles lois ainsi que d'organismes chargés de veiller à leur application (OCDE, 2006). Il faut cependant noter que ces lois assurent une protection

sur un territoire particulier, sans portée réelle – ou presque – lorsque les données se trouvent dans un autre pays.

2.1 Directive de l'OCDE

En 1980, l'OCDE propose de grands barèmes de protection de la vie privée communs à ses membres en espérant qu'ils servent de fondement au niveau mondial. Elle publie les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*. Ces lignes directrices « représentent un consensus international sur des orientations générales concernant le recueil [la collecte] et la gestion d'informations de caractère personnel » (OCDE, 2001:7). Elles inspirent d'ailleurs les lois de protection de la vie privée, notamment au Canada, en Australie et en Nouvelle-Zélande. Un des grands principes des lignes directrices concerne les limites à l'utilisation, à la divulgation et à la conservation des données. S'ajoutent à cela la spécification des finalités pour lesquelles sont recueillis des renseignements et les restrictions de collecte d'information qui ne serait pas nécessaire à l'objectif annoncé. Une partie de ces lignes directrices définit les principes concernant la libre circulation des données et les restrictions légitimes applicables à l'échelle internationale. Ces principes stipulent que « les pays membres devraient prendre en considération les conséquences pour d'autres pays membres d'un traitement effectué sur leur propre territoire et de la réexportation des données à caractère personnel » (OCDE, 2001:18). Le document de l'OCDE indique :

> Un pays membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays membre ne prévoit pas de protection équivalente (OCDE, 2001:19).

Cependant, la protection de la vie privée ne devrait pas servir de prétexte à la création d'obstacles administratifs qui limiteraient la circulation transfrontière des données vers des États qui partagent les mêmes exigences en la matière (OCDE, 2001).

En 1985, les États membres de l'OCDE adoptent la *Déclaration sur les flux transfrontières de données*. Ils réaffirment ainsi leur préoccupation à l'égard des problèmes soulevés par le flux transfrontière de données et leur désir de trouver des solutions communes. Cette déclaration vise à préciser l'esprit général dans lequel seront abordés les problèmes. Elle cible trois types de flux transfrontières de données : les flux de données liés à des activités de commerce international, les flux internes aux entreprises et les services d'information automatisés.

Un quart de siècle plus tard, l'OCDE constate que la préoccupation est toujours présente chez ses membres qui collaborent avec d'autres acteurs et certains pays à évaluer les pressions économiques et technologiques qui pourraient présenter des risques pour la vie privée (OCDE, 2006). Dans le *Rapport sur l'application transfrontière de la législation relative à la vie privée*, l'OCDE souligne « le besoin d'une approche plus globale et méthodique pour une coopération pour la mise en application des lois transfrontières régissant la vie privée » (OCDE, 2006:2). On y insiste sur l'importance d'une « action au niveau international destinée à remédier aux problèmes que pose l'application efficace des législations [de protection de la vie privée] dans un monde où les flux de données internationaux sont généralisés et continus » (OCDE, 2006:3). Le Rapport fait ressortir une importante lacune en matière de protection de la vie privée dans le contexte de flux transfrontières de données. Malheureusement, les instruments régionaux tels que les lignes directrices de l'APEC (Coopération économique Asie-Pacifique) et certains mécanismes moins formels issus des rencontres internationales relatives à la protection des données visant à faciliter la coopération transfrontière en matière de protection de la vie privée n'ont pas de portée internationale. Reste encore à trouver une forme de coopération transfrontière pour faire appliquer la législation sur la vie privée de manière plus globale (OCDE, 2006).

2.2 Directive de 1995 de l'Union européenne

En octobre 1995, le Parlement et le Conseil européens ont adopté la Directive de 1995 visant à protéger les données à caractère personnel et les droits et libertés des personnes, tout en facilitant la circulation de ces données à l'intérieur de l'Union européenne.

Depuis l'instauration de cette Directive, le transfert de données à caractère personnel dans les secteurs public et privé peut se faire sans contrainte entre les pays membres de l'Union européenne puisque chacun a transposé dans son droit national cette Directive en vue de protéger les renseignements personnels et les droits et libertés de la personne (CNIL, 2008). La Commission européenne veille à l'application de cette Directive lors des transferts de données vers des pays tiers. Le chapitre IV de la Directive porte expressément sur le transfert de données à caractère personnel vers ces autres pays. Les transferts de données sont permis seulement vers un pays tiers qui assure « un niveau de protection adéquat » du fait de sa législation interne ou de ses engagements internationaux. Après analyse de différents facteurs – nature des données, finalité, traitement envisagé, pays de destination finale et règles de droit en vigueur dans ce pays – la Commission européenne détermine si le niveau de protection est adéquat et correspond aux exigences de la Directive de 1995.

Lorsque les lois d'un pays tiers n'offrent pas un niveau de protection adéquat, des mesures sont prises en vue d'empêcher le transfert de données vers ce pays. La Commission peut néanmoins engager des négociations avec le pays tiers afin de

remédier à la situation. Sous certaines conditions, il est possible, dans des cas particuliers, qu'un transfert de données à caractère personnel puisse être autorisé en l'absence de protection adéquate. Cette situation peut se produire si « le transfert [est] nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice » (Directive 95/46/CE, chap. IV, art. 26, 1-d).

Un État qui autorise un transfert de données sans avoir l'assurance d'un niveau de protection adéquat doit toutefois conclure avec le responsable du traitement une entente qui inclut des garanties « au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants » (Directive 95/46/CE, chap. IV, art. 26, 2). L'État concerné doit aviser les autres États membres, et la Commission, des autorisations qu'il accorde ainsi.

Certains pays membres de l'EEE (Espace économique européen), dont l'Islande, le Liechtenstein et la Norvège, ont transposé la Directive de 1995 dans leur droit national. Leurs lois sont ainsi considérées comme équivalentes à celles des pays de l'Union européenne.

Afin de veiller à la sécurité des renseignements à caractère personnel dans les pays où les États membres de l'Union européenne souhaitent transférer des données et dont la législation n'est pas jugée équivalente, la Commission européenne a prévu un mécanisme d'adéquation des lois locales. La Suisse, le Canada, l'Argentine, les îles de Jersey et Guernesey et l'Île de Man se sont vus reconnaître un niveau de protection adéquat.

Concernant le Canada, la décision d'adéquation rendue en décembre 2001 porte uniquement sur la loi fédérale sur la protection des renseignements personnels et les documents électroniques du 13 avril 2000 (CNIL, 2008:14). Le Québec ne fait pas partie des destinations vers lesquelles le flux transfrontière de données est autorisé sans examen ou entente préalable. Il faut souligner que, compte tenu du partage des compétences au Canada, les provinces ont leurs propres lois en la matière, mais elles ne bénéficient pas automatiquement de la reconnaissance d'un niveau de protection adéquat par la Commission européenne.

La reconnaissance d'adéquation autorise le transfert de données vers des destinataires établis dans des pays tiers, sans formalités particulières (contrat, règles internes, etc.) pour encadrer le flux de données transfrontière (CNIL, 2008). Dans ce cas, les organisations souhaitant transférer des renseignements n'ont pas besoin non plus de consulter les organismes de contrôle institués dans les pays membres de l'Union européenne et qui veillent à protéger la vie privée et les libertés dans un monde interconnecté.

Le groupe de travail « Article 29 » de la Directive

La Directive de 1995 a mis en place un organe consultatif indépendant communément appelé groupe de travail « Article 29 » (le G29) – où se retrouvent les représentants des organes de contrôle des États membres – concernant les questions de protection des personnes à l'égard du traitement des données à caractère personnel. À la demande de la Commission européenne, le G29 émet des avis relatifs au « niveau de protection dans la Communauté européenne et dans les pays tiers » (Directive 95/46/CE, 1995).

Le G29 s'est notamment prononcé sur le transfert obligatoire des données des dossiers passagers (Passenger Name Record – PNR) aux autorités américaines en vue de confronter l'identité des voyageurs vers les États-Unis avec une liste de présumés terroristes. Cette exigence des États-Unis au sujet du transfert de renseignements à caractère personnel aux fins de la lutte contre le terrorisme allait pourtant à l'encontre de la Directive de 1995, alors que les lois des États-Unis en matière de protection des renseignements personnels et de la vie privée ne sont pas reconnues de niveau adéquat (24 juin 2008; 5 décembre 2007; 17 août 2007). Afin de remédier à ce problème, l'Union européenne a décidé de mettre en place à son tour un système PNR en tant que composante de sa stratégie antiterrorisme.

En outre, le G29 a récemment émis des avis concernant le standard international pour la protection des renseignements personnels de l'AMA (Agence mondiale antidopage) (6 avril 2009). Cela fait suite à un premier avis qui portait sur le « projet de norme internationale de protection de la vie privée du code mondial antidopage », adopté en août 2008.

2.3 *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada

Au niveau fédéral canadien, deux lois protègent la vie privée. La *Loi sur la protection des renseignements personnels* s'applique au secteur public, c'est-à-dire aux ministères, organismes et sociétés d'État. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) vise les organisations du secteur privé qui recueillent, utilisent et communiquent des renseignements personnels aux fins d'une activité commerciale[7].

Ces deux lois ne sont pas en vigueur dans les provinces qui ont établi leurs propres lois en matière de protection des renseignements personnels et de la vie privée dans les secteur public et privé lorsque celles-ci ont été déclarées « essentiellement similaires »[8]

[7] Selon la loi, une activité commerciale est définie comme « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature » (CPVP, 2008:8).

[8] Pour être reconnue essentiellement similaire, une loi provinciale ou territoriale doit incorporer les dix principes de la loi fédérale, fournir un mécanisme indépendant et efficace de surveillance et de recours avec

à la loi fédérale par le gouvernement du Canada. Le décret d'exclusion visant des organisations de la province de Québec, publié le 19 novembre 2003, vient confirmer la préséance de la loi québécoise dans ce domaine. La Colombie-Britannique et l'Alberta jouissent de cette même exclusion en raison de l'existence de lois dans ce domaine. En Ontario, le caractère d'équivalence concerne seulement les dépositaires de renseignements sur la santé (L.O. 2004, c. 3). Les lois fédérales prédominent seulement dans les cas où « 1) l'organisation est une installation, un ouvrage, une entreprise ou un secteur d'activité de compétence fédérale; 2) les renseignements personnels sont communiqués en dehors de la province dans le cadre d'une activité commerciale » (CPVP, 2008:1).

La LPRPDÉ comporte une section qui traite de la protection des renseignements personnels à l'étranger dans les cas d'impartition ou d'autres activités transfrontalières. Néanmoins, selon la Commissaire à la protection de la vie privée du Canada (CPVP, 2008:i), « les progrès en technologie de l'information et le désir de soutenir la concurrence à l'échelle mondiale » complexifient « les défis liés à la protection de la vie privée ».

Une stratégie et des politiques fédérales ont été élaborées afin d'encadrer les flux transfrontières de données. La stratégie met de l'avant la protection de la vie privée comme droit fondamental de la personne (CPVP, 2006). Néanmoins, en 2006, le Commissariat réclamait la révision de la *Loi sur la protection des renseignements personnels,* entrée en vigueur en 1983. Il soulignait alors que cette la loi accuse un retard déplorable en ce qui concerne les questions liées à la mondialisation et à l'impartition à grande échelle du traitement et du stockage de renseignements personnels (CPVP, 2006).

Au Canada, les préoccupations entourant la protection de la vie privée dans le contexte des activités transfrontalières ont été mises à rude épreuve par les demandes d'information en provenance des autorités des États-Unis invoquant les pouvoirs conférés par le *USA PATRIOT Act.* Quelques cas ont fait l'objet d'une enquête par le Commissariat à la protection de la vie privée du Canada.

En vertu de la loi, une organisation est autorisée à « communiquer des renseignements personnels à un tiers aux fins de traitement » sous trois conditions. 1- « L'organisation demeure responsable des renseignements personnels conformément à la LPRPDÉ, peu importe où sont les données »; elle a le devoir de les protéger. 2- L'organisation prévoit les mesures nécessaires afin de « garantir que l'information traitée par un tiers bénéficiera du même niveau de protection ». 3- L'organisation indique « qu'elle a recours à un fournisseur "américain" et avise ses clients du risque que leurs

des pouvoirs d'enquête et « restreindre la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes ». Une loi essentiellement similaire est donc reconnue comme étant égale ou supérieure à la loi fédérale pour ce qui est du degré et de la qualité de la protection de la vie privée offerte. La loi fédérale représente un seuil minimum » (Canada, *Gazette du Canada*, partie I, Vol. 136, n° 31 – le 3 août 2002:2388).

renseignements personnels puissent être communiqués de façon légale aux autorités "américaines" » (Kosseim, 2006:2).

Selon les principes de la « common law », la loi est applicable aux personnes, aux choses et aux activités qui se situent à l'intérieur des frontières canadiennes (Kosseim, 2006:5). Patricia Kosseim, avocate générale du CPVP, voit là un problème. Elle s'interroge, entre autres, à propos des situations où il est difficile d'identifier l'instance responsable de la protection des données, notamment à cause d'Internet, qui peut rendre plus problématique la localisation physique des renseignements. Elle préconise la mise au point de dispositions de portée mondiale et souligne quelques initiatives auxquelles participe le Canada.

Outre la stratégie publiée en 2006 qui visait à répondre aux préoccupations liées aux flux de données transfrontières, particulièrement en rapport avec le *USA PATRIOT Act*, les autorités canadiennes et américaines examinent la possibilité d'élaborer des « ententes spéciales d'assistance judiciaire mutuelle qui permettraient de faciliter la tenue d'enquêtes et l'application des lois sur la protection des données par delà les frontières » (Kosseim, 2006:6).

2.4 *Loi sur la protection des renseignements personnels dans le secteur privé du Québec*

Au Québec, deux lois régissent la protection des renseignements personnels dans le secteur public et le secteur privé. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1), communément appelée la Loi d'accès, jumelle l'accès à l'information et la protection des renseignements personnels. La *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) couvre, comme son nom l'indique, le secteur privé. Cette loi établit des règles à l'égard de la collecte, de l'utilisation et de la communication des renseignements personnels recueillis par une entreprise ou un ordre professionnel à des fins commerciales dans la province. Elle a été déclarée essentiellement similaire à la loi fédérale. Par conséquent, elle a préséance au Québec, sauf pour les exceptions mentionnées précédemment (CPVP, 2008).

La loi québécoise visant le secteur privé comporte un article sur le transfert de données vers un pays tiers (L.R.Q. c. P-39.1, art.17). Ainsi, toute entreprise qui souhaite transférer à l'extérieur du Québec des renseignements personnels afin de les conserver, de les utiliser ou de communiquer les renseignements pour son compte doit respecter deux clauses. Premièrement, elle doit s'assurer que ces renseignements ne seront pas utilisés, sans le consentement des personnes concernées, à d'autres fins que celles pour lesquelles ils ont été recueillis, sauf dans quelques cas d'exception stipulés dans la loi, notamment en matière criminelle. Deuxièmement, elle doit accorder aux personnes

concernées la possibilité de retirer leurs renseignements nominatifs d'une liste si cette dernière est utilisée à des fins de recherche commerciale ou philanthropique.

Si un doute existe quant aux conditions de sécurité des renseignements personnels, une entreprise ne doit pas les communiquer ou les confier à un organisme à l'extérieur du Québec.

Règle générale, la divulgation de renseignements à des tiers nécessite le consentement de la personne concernée. Les quelques exceptions sont habituellement justifiées par des situations d'urgence, d'enquête ou d'infraction et à des fins de sécurité d'une personne ou d'un groupe de personnes lorsqu'il existe un motif raisonnable de croire qu'elles sont en danger (L.R.Q. c. P-39.1, art.18).

La banque de données de l'Agence mondiale antidopage

Quant aux difficultés qui peuvent se présenter en matière de protection des renseignements personnels et de la vie privée lors de transferts internationaux, un litige impliquant une organisation internationale basée au Québec s'avère particulièrement révélateur.

À quelques mois des Jeux olympiques d'hiver de Vancouver, la Commission européenne s'est interrogée à propos de la loi à laquelle est assujettie l'AMA (l'Agence mondiale anti-dopage). Cette agence internationale indépendante, sans but lucratif, a été créée en 1999 afin de promouvoir, de coordonner et de superviser la lutte contre le dopage dans le sport. Son siège est à Lausanne, en Suisse, et son bureau principal, à Montréal.

L'AMA est responsable de la base de données ADAMS, qui contient des informations à caractère personnel au sujet des athlètes. Ces informations sont transférées par l'AMA à d'autres organisations sportives de contrôle antidopage, principalement lors d'événements sportifs comme les Jeux olympiques ou des rencontres internationales, telles que la Coupe du monde de soccer. La Commission européenne a demandé au groupe de travail de « l'Article 29 » d'examiner le cas des données personnelles conservées par l'AMA dans sa base ADAMS et de déterminer la législation qui protège la vie privée et l'autorité responsable de la surveillance.

Le G29 s'est d'abord adressé au Commissariat à la protection de la vie privée du Canada. Ce dernier a précisé que l'AMA est considérée comme une organisation sans but lucratif et que, de ce fait, elle n'est pas assujettie à la loi fédérale sur la protection des renseignements personnels et les documents électroniques. Le Commissariat n'a pas, à ce stade, expliqué le partage des compétences avec les provinces canadiennes. Les autorités européennes ont alors estimé que le bureau de l'AMA à Montréal se trouvait dans un vide juridique et que, par conséquent, la vie privée des athlètes pouvait être menacée.

La Commission d'accès à l'information (CAI) du Québec est intervenue pour clarifier la situation et a présenté sa position au G29. Selon la CAI, la loi québécoise s'applique aux activités de l'AMA sur son territoire; l'AMA ne fait donc pas face à un vide juridique en matière de protection des renseignements personnels et de la vie privée. Plus encore, précise le président de la Commission d'accès à l'information, la législation du Québec et celle du Canada sont « conformes aux principes fondamentaux de protection de la vie privée et s'inspirent largement de la Directive européenne 95/46/CE portant sur la protection des données à caractère personnel » (Saint-Laurent, 2009:2).

L'origine de cette confusion remonte au moment où la Commission européenne a reconnu adéquate la loi fédérale sur la protection des renseignements personnels et les documents électroniques sans prendre en considération le partage des compétences entre les provinces et le gouvernement fédéral.

Ce problème d'application de la loi associée au territoire où se trouvent les renseignements comporte deux dimensions. En premier lieu, la Commission européenne doit déterminer quelle loi est applicable dans un contexte fédéral. Elle doit aussi évaluer si cette loi, en l'occurrence la loi québécoise, protège suffisamment les renseignements personnels détenus au Québec et par conséquent la vie privée des athlètes. Les autorités de protection des renseignements personnels et de la vie privée du Québec répondent par l'affirmative. Cette garantie est valable tant et aussi longtemps que les données demeurent en sol québécois. La seconde dimension du problème se dessine lorsque les renseignements sont transférés à l'étranger en fonction des événements sportifs. C'est en principe la loi du pays où ils sont acheminés qui doit les prendre en charge. Le G29 émettra prochainement un avis à la Commission européenne qui rendra alors sa décision sur le dossier concernant l'assujettissement de l'AMA à la loi québécoise.

2.5 *Privacy Act* et *USA PATRIOT Act* des États-Unis

Le *Privacy Act* de 1974 (The Privacy Act of 1974, 5 U.S.C. § 552a) est la principale loi qui régit l'usage, par le gouvernement des États-Unis, des renseignements personnels des citoyens et résidents permanents contenus dans des bases de données gouvernementales fédérales. Cette loi établit les règles de collecte, de conservation, d'utilisation et de diffusion des données à caractère personnel dans le seul secteur public. Elle dicte aussi les obligations des institutions gouvernementales qui détiennent des bases de données. Ces dernières doivent notamment enregistrer leurs bases de données dans le Registre fédéral. Sauf dans quelques exceptions, elles ne peuvent pas divulguer ces renseignements sans le consentement écrit de la personne concernée. Cette loi restreint en outre le partage des données entre les organisations, qui doivent établir des ententes particulières à cette fin. De plus, le citoyen doit disposer d'un moyen de demander accès à ses données personnelles et à leur modification. Cette loi permet

aux citoyens d'engager des poursuites contre le gouvernement s'ils pensent que leurs droits ont été violés.

La loi sur la vie privée fédérale ne s'applique pas aux gouvernements des États fédérés, ni aux municipalités, en conséquence de quoi ces derniers doivent avoir leurs propres lois concernant les bases de données de renseignements personnels. Certains États possèdent des lois qui visent à protéger la vie privée dans des domaines précis, par exemple les dossiers bancaires, scolaires ou médicaux.

Il n'existe pas de loi particulière sur la protection des renseignements personnels dans le secteur privé aux États-Unis. Seule la Federal Trade Commission (FTC), qui a notamment le mandat de protéger les consommateurs, veille à faire respecter leur vie privée par les entreprises qui recueillent, utilisent et archivent des renseignements personnels.

En 1998, les États-Unis ont entrepris des négociations avec l'Union européenne afin d'obtenir un accord qui autoriserait les flux de données transfrontières malgré la non-adéquation des lois des États-Unis en matière de protection des renseignements personnels avec la Directive européenne de 1995. En 2000, l'accord de « Safe Harbor » ou « Sphère de sécurité » a été conclu entre Washington et l'Union européenne. Ainsi, les entreprises américaines qui adhèrent, sur une base volontaire, aux sept principes de protection des renseignements personnels et de la vie privée de la « Sphère de sécurité » sont admissibles aux flux transfrontières de données en provenance de pays membres de l'Union européenne[9]. Ces principes ont été négociés par la Commission européenne et le ministère du Commerce des États-Unis et se basent sur la Directive de 1995. Le contrôle du respect de ces principes par les entreprises américaines est à l'occasion remis en question, notamment par la Commission européenne qui a demandé, en 2004, une meilleure surveillance de la part des autorités américaines (Fuster, De Hert et Gutwirth, 2008; Privacy International 2007a,b).

En octobre 2001, l'entrée en vigueur du *USA PATRIOT Act* a modifié plus de quinze lois importantes aux États-Unis. En général, le *USA PATRIOT Act* a préséance sur les autres lois. Il permet, entre autres, aux autorités gouvernementales fédérales des États-Unis d'avoir accès à des renseignements personnels concernant des étrangers, à l'insu de ces derniers « si l'information se trouve physiquement sur le territoire des États-Unis » ou si les entreprises basées aux États-Unis ont directement accès aux renseignements, notamment par voie électronique (SCT, 2006:2). Cette loi a, par exemple, modifié le *U.S. Foreign Intelligence Surveillance Act*, de sorte que le Federal Bureau of Investigation (FBI) peut demander une ordonnance de la cour « en vue d'obtenir des dossiers, des papiers, des documents et d'autres éléments dans le cadre

[9] Selon un de ces principes, les entreprises qui adhèrent à la « Sphère de sécurité » peuvent aussi transférer des données vers des tierces parties à condition que ces dernières soient assujetties à la Sphère de sécurité, à la Directive européenne de 1995 ou à une loi reconnue adéquate par cette Directive.

d'enquêtes sur des activités terroristes ou des activités clandestines de renseignement » (SCT, 2006:11).

Quant aux renseignements personnels détenus à l'étranger et auxquels les autorités américaines souhaiteraient accéder afin d'assurer la sécurité aux États-Unis ou de poursuivre les objectifs de lutte contre le terrorisme, des démarches peuvent être entreprises afin d'obtenir cet accès. Il faut alors démontrer que les renseignements se trouvent aussi sous la responsabilité d'une entité des États-Unis (Privacy International, 2008). Le cas du transfert des dossiers passagers (PNR) en constitue un exemple. Les États-Unis ont demandé aux compagnies aériennes européennes, sous menace de pénalités financières ou d'interdiction de survoler et d'atterrir sur leur territoire, de leur fournir les données personnelles contenues dans les dossiers passagers de toute personne à destination des États-Unis ou transitant par le pays. Ce transfert a été jugé illégal aux yeux du Parlement européen en mai 2006.

La quête d'information par des autorités des États-Unis à des fins de prévention d'actes terroristes après l'adoption du *USA PATRIOT Act* est impressionnante dans divers domaines. Le cas de SWIFT (Society of Worldwide Interbank Financial Telecommunications) illustre bien la détermination des autorités américaines d'accéder à de telles données pour des motifs de sécurité nationale. SWIFT est une coopérative qui traite les transferts bancaires internationaux. Elle est basée en Belgique, et par conséquent, assujettie aux lois de ce pays. À des fins de sécurité, l'entreprise conserve un double des données dans l'un de ses centres d'opérations aux États-Unis. À la suite des attentats du 11 septembre 2001 et en raison de la mise en place de nouvelles exigences des États-Unis en vue de lutter contre le terrorisme, SWIFT a été contrainte de divulguer au US Treasury Department (UST) les informations concernant les transactions bancaires de ses clients, incluant des renseignements personnels. SWIFT a tenté de limiter la circulation de l'information et de conserver un certain contrôle. Cette société a notamment demandé que les renseignements soient consultés uniquement en cas d'enquête sur le terrorisme et que certaines clauses de confidentialité soient préservées, mais elle ne s'est pas opposée à la divulgation des renseignements. SWIFT n'a pas non plus informé les autorités de protection des renseignements de l'Union européenne de ces transferts de données.

Cette façon de procéder allait à l'encontre de la Directive européenne. Après quelques examens et avis, notamment par le G29, un accord provisoire a été conclu en juin 2007 entre l'Union européenne et les États-Unis concernant le transfert des données de SWIFT. La société a adhéré à la Sphère de sécurité, fait étonnant puisqu'il s'agit d'une entreprise européenne et que la Sphère de sécurité est destinée aux entreprises des États-Unis afin qu'elles soient admissibles au transfert de renseignements en provenance de l'Europe. Le 11 février 2009, le Parlement européen a rejeté cet accord concernant le transfert des données bancaires afin de privilégier le respect de la vie privée.

2.6 Qu'en est-il ailleurs dans le monde ?

Les pays occidentaux se sont majoritairement dotés de lois et se soucient de protection des renseignements personnels et de la vie privée. D'autres régions du monde ne partagent pas les mêmes préoccupations à ce sujet.

Bien qu'elles ne soient pas gage de sécurité absolue en matière de protection des renseignements personnels et de la vie privée, les lois nationales imposent tout de même des contraintes aux États vers lesquels peuvent être transférées de telles données. Les mesures de sécurité mises en place par un État peuvent susciter des discussions et des négociations avec les autres pays, voire empêcher le transfert de données. Elles favorisent la réflexion sur les façons de gérer les données et de protéger la vie privée et peuvent entraîner des modifications législatives. L'exemple du Pakistan illustre bien ce type de situation. D'une part, les législateurs du pays indiquent que la vie privée est suffisamment protégée par la Constitution qui puise ses principes dans l'Islam. D'autre part, le gouvernement pakistanais considère qu'il ne faciliterait pas le développement du commerce avec des pays de cultures différentes (essentiellement occidentaux) s'il ne tenait pas compte des exigences de la Directive européenne de 1995; d'où l'importance accordée à satisfaire et rassurer les pays de l'Union européenne par l'élaboration d'un projet de loi sur la protection des données (Hayat, 2007).

Au cours des dernières années, l'Inde a abrité de nombreux centres d'appels répondant à la demande d'impartition de services d'organisations occidentales; pourtant, ce pays n'a pas de loi spécifique en matière de protection des renseignements personnels. Il s'est néanmoins doté de plusieurs lois qui visent à protéger ces renseignements. L'utilisation des données est régie par trois lois : l'*Information Technology Act 2000* (modifié par l'*Information Technology Amendment Act 2008)*, l'*Indian Copyright Act 1957* et le *Trademarks Act 1999*. Ces lois ont permis au Commissaire à l'information du Royaume-Uni de reconnaître l'Inde comme offrant une « protection adéquate » des données sur son territoire (Haden, 2006; Jacob, 2009). Compte tenu des exigences des pays développés, notamment au sein de l'Union européenne et afin de faciliter la sous-traitance, l'Inde a décidé de s'aligner sur les pays qui ont légiféré sur le sujet. En 2008, cet État a donc inclus dans sa loi sur les technologies de l'information une section visant la protection des données (Bond et Bange, 2009). L'Inde s'apprêterait à édicter une loi sur la protection des données personnelles. Pour des raisons politiques, semble-t-il, le projet de loi demeure en suspens (Gunasekara, 2009; Privacy International, 2009).

Une étude réalisée dans six pays d'Asie (Bangladesh, Inde, Malaisie, Pakistan, Philippines et Thaïlande) souligne que les mesures de protection des renseignements personnels et de la vie privée mises en place récemment visent en général à répondre aux exigences des États-Unis ou de l'Union européenne dans le but de favoriser les activités commerciales. Elles n'améliorent pas nécessairement les droits des citoyens (Privacy International, 2009). Dans la majorité de ces pays, la protection de la vie privée est définie dans la Constitution. Le défi réside donc dans la transposition de ces principes dans le système légal. La nécessité s'impose d'évaluer plus en profondeur les

lois en vigueur, notamment quant à leur définition de « renseignement personnel », de ce qui porte atteinte à la vie privée et de la portée des mécanismes de plaintes, ainsi que de déterminer le secteur auquel elles s'appliquent.

L'APEC s'intéresse particulièrement aux questions de vie privée en Asie, entre autres dans l'optique de favoriser le commerce international et les ententes d'impartition avec les pays de cette région. C'est pourquoi, afin de promouvoir de meilleures normes internationales, elle a élaboré des lignes directrices concernant l'adoption d'un cadre international qui pourrait améliorer la protection des renseignements personnels et de la vie privée lors des flux transfrontières de données (APEC, 2005; Conférence mondiale des Commissaires, 2008; Privacy International, 2007a).

3. Cheminer vers une protection internationale des renseignements

La portée des lois de protection des renseignements personnels et de la vie privée est principalement intra-étatique. Quelques éléments des lois en la matière ont une portée internationale, mais ils servent surtout à autoriser ou non un transfert de données vers l'étranger.

Un examen des lois actuelles permet de voir qu'effectivement, elles accusent un retard lorsqu'il est question de flux transfrontières. Les lois ne permettent pas d'assurer la même protection quand les renseignements personnels quittent leur territoire d'origine, et moins encore dans un contexte de lutte contre le terrorisme où, au nom de la sécurité, les autorités responsables tentent d'obtenir un maximum de renseignements sur les individus, quels qu'ils soient. Ce ne sont plus seulement les données personnelles des suspects qui sont scrutées à la loupe – la demande des dossiers de passagers aériens (PNR) témoigne bien de cette recherche de sécurité.

Les mesures actuelles de protection des renseignements personnels et de la vie privée soulèvent énormément d'interrogations chez les acteurs concernés par les flux transfrontières de données. Elles exigent beaucoup de travail en vue de la transmission de données à l'étranger. Dans chaque cas, ou presque, il faut évaluer si les données transférées auront une protection suffisante. Plus encore, il s'agit de voir si elles auront le même niveau de protection que dans l'État d'où elles proviennent. Nombreux sont les exemples où les commissaires à l'information et à la protection de la vie privée sont interpellés afin de se prononcer sur la sécurité du transfert de renseignements personnels à l'étranger.

Certes, les pays tentent d'encadrer les flux transfrontières de données et de définir en commun des mesures visant des situations de plus en plus fréquentes, comme

l'impartition de services ou les demandes d'autorités gouvernementales au nom de la lutte contre le terrorisme. Toutefois, ces procédures exigent beaucoup de temps et permettent difficilement de suivre le rythme des flux. Les données peuvent avoir parcouru beaucoup de chemin avant qu'une décision ne soit appliquée.

Aucune entente internationale n'existe afin de protéger la vie privée et les renseignements personnels. Aucune institution n'est mandatée pour faire respecter des normes internationales de base. C'est pourquoi, en cette actuelle phase de mondialisation et sous l'effet des nouvelles technologies de l'information et des communications, des voix s'élèvent en faveur d'une gouvernance mondiale de la protection des renseignements personnels. Des revendications proviennent de groupes de défense de la vie privée comme EPIC (Electronic Privacy Information Center) et Privacy International. Les autorités de contrôle de la protection des renseignements personnels se sont d'ailleurs prononcées sur cette préoccupation. Lors des dernières conférences internationales des Commissaires à la protection des données et à la vie privée, des appels ont été lancés en faveur d'une meilleure protection, notamment par l'adoption d'un instrument juridique universel contraignant (2008) et de normes internationales (2009). Une déclaration d'appui de la société civile sur le besoin de « standards mondiaux de respect de la vie privée dans un monde globalisé » a été déposée à la 31^{e} Conférence des Commissaires, en novembre 2009. Les Commissaires à la protection des données et à la vie privée ont commencé à travailler à l'élaboration de standards internationaux qui seraient contraignants.

Conclusion

La libéralisation des échanges et les technologies de l'information ont grandement favorisé les flux transfrontières de données. Cette possibilité de transfert de renseignements personnels à l'étranger soulève, chez la majorité des acteurs concernés par cette situation, des inquiétudes quant à la protection qu'offrent les lois actuelles en matière de vie privée. Les chercheurs et responsables de la protection des renseignements conviennent que ces lois, bien qu'utiles dans un pays donné, ont une portée limitée à l'étranger. Comme l'affirme Gunasekara (2007), les flux transfrontières de données sont insuffisamment couverts par les normes actuelles de protection de la vie privée. « Il existe un espace considérable pour une approche plus globale et plus systématique en faveur d'une coopération transfrontière pour faire appliquer la législation sur la vie privée » (OCDE, 2006:4). Ce point saillant du récent rapport de l'OCDE fait également ressortir les lacunes en matière de protection de la vie privée dans le contexte de flux transfrontières de données. Les Commissaires à la protection des données et à la vie privée revendiquent l'amélioration de cette situation et ils y œuvrent depuis quelques années déjà.

À l'échelle de la planète, il devient de plus en plus difficile de protéger les renseignements personnels et la vie privée par des lois et règlements édictés dans chaque État. Il faudra trouver le moyen de rendre plus efficaces les mesures de protection de la vie privée relativement aux flux transfrontières de données qui, vraisemblablement, n'iront pas en diminuant avec la tendance au « cloud computing ». Pour ce faire, il faudra analyser la question sous un angle différent de celui sous lequel les États et gouvernements ont jusqu'à présent perçu le problème et défini ces lois. Comme le réclament Martin et Rabina (2009), les gouvernements doivent désormais penser à protéger les citoyens à l'égard de ce droit tant à l'intérieur qu'à l'extérieur de leur pays. Par analogie, il s'avère pertinent de voir si les mesures de protection des renseignements personnels et de la vie privée peuvent s'inspirer de la lutte des États-Unis contre le terrorisme, laquelle s'appuie sur des « mécanismes » de la mondialisation pour protéger le pays. Dans cet ordre d'idée, il faudra également se pencher sur la question idéologique et éthique de la limite à tracer entre la protection de la vie privée et le besoin de sécurité nationale et internationale.

Enfin, il convient aussi d'examiner comment arriver à un accord international tout en tenant compte des différences légales, culturelles et politiques. Néanmoins, la recherche seule ne sera pas suffisante. L'appel à la coopération et à l'élaboration de normes et standards internationaux par les acteurs concernés par la protection des renseignements personnels et de la vie privée devra être entendu. La volonté des dirigeants des pays leaders en la matière s'avèrera aussi nécessaire à l'avancement d'un tel chantier.

Bibliographie

APEC - Coopération économique Asie-Pacifique. 2005. *APEC Privacy Framework.* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf

Bond**,** Robert and Vinod Bange**.** 2009. «New Data Protection Laws for India», *Speechly Bircham Inform: IP, Technology & Commercial*, 27 April. http://ca.linexlegal.com/index.php

Canada. 2002. « Loi sur la protection des renseignements personnels et les documents électroniques : Processus de détermination du caractère « essentiellement similaire » d'une loi provinciale par le gouverneur en conseil », *Gazette du Canada*, Partie I, Vol. 136, n° 31, 3 août, p. 2385-2389. http://www.gazette.gc.ca/archives/p1/2002/2002-08-03/pdf/g1-13631.pdf

Caruana, Mireille M. and Joseph A. Cannataci. 2007. "European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States", *Information & Communications Technology Law.* Vol. 16, n° 2, June, p. 99.

Chandler, Jennifer. 2009. "Privacy Versus National Security: Clarifying the Trade-Off", *in* Kerr, Ian, Valerie Steeves and Carole Lucock (Eds), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, Chap. 7, April, p. 121-138.

Conférence internationale des Commissaires à la protection des données et à la vie privée. 2009. *Proposition de résolution concernant le renforcement de la coopération internationale en matière de protection des données et de la vie privée,* 31e Conférence, Madrid, 4 au 6 novembre.

Conférence mondiale des Commissaires à la protection des données et de la vie privée. 2008. *Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles*, 30e Conférence, Strasbourg, 15-17 octobre.

Comeau, Paul-André. 2002. « Un modèle québécois en matière d'accès à l'information et de protection des renseignements personnels», *in* L'observatoire de l'administration publique, *Coup d'œil*, Vol. 8, n° 3, octobre, p. 8-11.

CNIL - Commission nationale de l'informatique et des libertés. 2008. *Transferts de données à caractère personnel vers des pays non membres de l'Union européenne*, juin.
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf

CPVP - Commissariat à la protection de la vie privée du Canada. 2009. *Traitement transfrontalier des données personnelles : Lignes directrices.*
http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.pdf

CPVP - Commissariat à la protection de la vie privée du Canada. 2008. *Tracer le chemin : Principaux développement au cours des sept premières années d'application de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ).*
http://www.priv.gc.ca/information/pub/lbe_080523_f.pdf

CPVP - Commissariat à la protection de la vie privée du Canada. 2006. *La commissaire à la protection de la vie privée du Canada appuie la nouvelle stratégie du gouvernement fédéral pour régir la circulation transfrontalière de renseignements personnels*, Communiqué, Ottawa, 6 avril. (Consulté le 18 janvier 2010).
http://www.priv.gc.ca/media/nr-c/2006/nr-c_060406_f.cfm

EPIC – Electronic Privacy Information Center. --. *The Privacy Act of 1974*. (Consulté le 20 janvier 2010).
http://epic.org/privacy/1974act/

Fuster, Gloria González, Paul De Hert and Serge Gutwirth. 2008. "SWIFT and the Vulnerability of Transatlantic Data Transfers", *International Review of Law, Computers & Technology.* Vol. 22, n° 1/2, March, p. 191-202.

Gunasekara, Gehan. 2007. "The "Final" Privacy Frontier? Regulating Trans-Border Data Flows", *International Journal of Law and Information Technology*, August, p. 1-33.

Haden, Belinda. 2006. "Data security and offshoring", *Journal of Direct, Data and Digital Marketing Practice***,** Vol. 7, n° 3; January-March, p. 266.

Hayat, Muhammad Aslam. 2007. "Privacy and Islam: From the Quran to Data Protection *in* Pakistan**",** *Information & Communications Technology Law*, Vol. 16, n° 2, p. 137 – 148.

Holder, James T. and David E. Grimes. 2007. "Government Regulated Data Privacy: The Challenge for Global Outsourcers", *Georgetown Journal of International Law*, Vol. 38, n° 3, Spring, p. 695-711.

Jacob, Shojan. 2009. «Data Protection Law in India » *Indlaw news.com*, Wednesday, december 23. (Consulté le 22 décembre 2009). http://www.indlawnews.com/display.aspx?4530

Karyda, Maria, Evangelia Mitrou and Gerald Quirchmayr. 2006. "A framework for outsourcing IS/IT security services", *Information Management & Computer Security*, Vol. 14, n° 5, p. 402-415.

Kosseim, Patricia. 2006. *La protection des renseignements personnels au Canada et à l'étranger*, Allocution, Sommet des avocats de société du Canada, Ottawa, 6 mars. http://www.priv.gc.ca/speech/2006/sp-d_060306_pk_f.cfm

Leonard, Thierry et Anthony Mention. 2008. "Transfert transfrontaliers de données: quelques considérations théoriques et pratiques", *in* Docquir, Pierre-François. 2008. *Actualités du droit de la vie privée*, chap.3, p. 89-137.

Martin, Shannon and Debbie Rabina. 2009. "National Security, Individual Privacy and Public Access to Government-Held Information: the Need for Changing Perspectives in a Global Environment", *Information & Communications Technology Law*, Vol 18, n° 1, p. 13 – 18.

McCullagh, Karen. 2009. "Protecting 'Privacy' Through Control of 'Personal' Data Processing: A Flawed Approach"**,** *International Review of Law, Computers & Technology***,** Vol. 23, n° 1/2, March, p. 13-24.

OCDE - Organisation de coopération et de développement économique. 2006. *Rapport sur l'application transfrontière de la législation relative à la vie privée*. http://www.oecd.org/dataoecd/4/54/37572078.pdf

OCDE - Organisation de coopération et de développement économique. 2001. *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*. http://browse.oecdbookshop.org/oecd/pdfs/browseit/9302012E.PDF

Ovenden, Sinead. 2009. "Data Protection and Third Parties: A Balancing Act", *Accountancy Ireland*, Vol. 41, n° 1, February, p. 50-52.

Poullet, Yves. 2007. «Comment appliquer les règles de protection des données aux transferts de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle ?», *Lex Electronica*, Vol. 12 n°1, Printemps. http://www.lex-electronica.org/articles/v12-1/poullet.pdf

Privacy International. 2009. *Privacy in Asia Final Report of Scoping Project*, November. http://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf

Privacy International. 2008. *PI Explains Risks to Census Data by Using U.S. Contractors Without Strong Protections*, 28 February, (Consulté le 18 janvier 2010). http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-561714

Privacy International. 2007a. *PHR2006 – Overview of Privacy*, 16 december. (Consulté le 18 janvier 2010).
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559474

Privacy International. 2007b. *PHR2006 – United States of America*, 18 december. (Consulté le 18 janvier 2010).
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559478

Saint-Laurent, Jacques. 2009. *Lettre du président de la Commission d'accès à l'information du Québec à Madame Jennifer Stoddart, Commissaire à la protection de la vie privée du Canada*, Objet : Agence mondiale anti-dopage (AMA), 3 avril 2009. (Consulté le 10 août 2009).
http://www.wada-ama.org/rtecontent/document/outgoing_letter_attachmt_SaintLaurent_ccm082751_reWADA.pdf

SCT- Secrétariat du Conseil du Trésor du Canada. 2006. *Protéger les renseignements personnels – Un impératif : La stratégie fédérale visant à répondre aux préoccupations suscitées par la USA PATRIOT Act et le flux de données transfrontière.*
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp-fra.pdf

Sommet de la Francophonie. 2006. *Déclaration de Bucarest*, XI^{e} Conférence des chefs d'État et de gouvernement des pays ayant le français en partage, Bucarest (Roumanie), les 28 et 29 septembre 2006.
http://inforoutes.francophonie.org/doc/txt-reference/decl-bucarest-2006.pdf

Stefanick, Lorna. 2007. "Outsourcing and Transborder Data Flows: the Challenge of Protecting Personal Information Under the Shadow of the USA PATRIOT Act", *International Review of Administrative Sciences*, Vol. 73, n^{o} 4, December, p. 531- 548.

The Public Voice. 2009. *Standards mondiaux de respect de la vie privée dans un monde globalisé*, Déclaration de la société civile Madrid, Espagne 3 novembre. http://thepublicvoice.org/madrid-declaration/fr/

Législation

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Union européenne.
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46

Loi de 2004 sur la protection des renseignements personnels sur la santé, L.O. 2004, c. 3, Ontario.
http://www.canlii.org/fr/on/legis/lois/lo-2004-c-3-ann-b/derniere/lo-2004-c-3-ann-b.html

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), L.C. 2000, ch. 5, Canada, À jour au 31 décembre 2009.
http://lois.justice.gc.ca/PDF/Loi/P/P-8.6.pdf

Décret d'exclusion visant des organisations de la province de la Colombie-Britannique, D.O.R.S./2004-220; voir aussi *Personal Information Protection Act*, S.B.C. 2003, c. 63.

Décret d'exclusion visant des organisations de la province d'Alberta, D.O.R.S./2004-219; voir aussi *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

Décret d'exclusion visant des organisations de la province de Québec, D.O.R.S./2003-374.
http://canadagazette.gc.ca/archives/p2/2003/2003-12-03/html/sor-dors374-fra.html

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1, Québec.
http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1, Québec.
http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html

The Privacy Act of 1974, 5 U.S.C. § 552a, États-Unis.
http://www.justice.gov/opcl/privacyact1974.htm

Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA PATRIOT Act) Act Of 2001, Public Law 107–56—OCT. 26, 2001.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

Le *Laboratoire d'étude sur les politiques publiques et la mondialisation* a été créé en 2004 par une entente de partenariat entre le Ministère des Relations internationales et l'ENAP. Le Laboratoire est un lieu de veille et d'analyse consacré à l'étude des effets de la mondialisation sur le rôle de l'État et sur les politiques publiques au Québec et sur les enjeux d'ordre culturel, économique, environnemental, de santé, d'éducation et de sécurité.

Relations internationales Québec

Directeur : Paul-André Comeau

Renseignements :
Karine Plamondon, technicienne en administration et information
Téléphone : (418) 641-3000 poste 6864
leppm@enap.ca

Les publications du Laboratoire peuvent être consultées sur le site internet :
www.leppm.enap.ca

Pour citer ce document :

TREMBLAY, Monica. Flux transfrontières de données et protection de la vie privée : une conjonction difficile. Québec, Laboratoire d'étude sur les politiques publiques et la mondialisation, ENAP, 2010. 29 p.

École nationale d'administration publique

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2010
Dépôt légal - Bibliothèque et Archives Canada, 2010

ISBN 978-2-923008-93-6 (version imprimée)
ISBN 978-2-923008-94-3 (PDF)