DEUXIÈME COMMISSION D'ÉTUDE

Droit et procédure civils

QUESTIONNAIRE 2010

QUESTIONS CIVILES LIÉES À LA PROTECTION DE LA VIE PRIVÉE
(PLUS PRÉCISÉMENT LORSQU'INTERNET EST EN JEU)

RAPPORT SOMMAIRE

INTRODUCTION

Le présent rapport sommaire a été rédigé à partir de 24 réponses au questionnaire. Les associations participantes des pays suivants ont soumis des rapports : l'Australie, l'Autriche, le Canada, l'Estonie, la Géorgie, l'Allemagne, l'Islande, l'Irlande, Israël, l'Italie, le Japon, le Kazakhstan, la Lituanie, le Luxembourg, le Maroc, la Pologne, le Portugal, la Slovénie, la Suède, la Suisse, la Tunisie, le Royaume-Uni et les États-Unis.

A. LOIS ET RÈGLEMENTS

1. Quelles lois régissent la protection de la vie privée dans votre système judiciaire? Existe-t-il des dispositions dans le *Code civil*, les lois ou la common law qui protègent les particuliers contre les atteintes à la vie privée?

Les associations de la plupart des pays ont souligné que le droit à la vie privée est explicitement inscrit dans leur constitution. Ailleurs, le droit à la vie privée a été interprété et reconnu comme un droit constitutionnel, établi par la jurisprudence. Ce droit constitutionnel est établi par des dispositions du *Code civil* ou de lois et par des revendications en common law. Par exemple, le *Code civil* général de l'Autriche traite du droit d'un individu à son nom, son domaine, sa sphère de vie privée et à l'honneur. Au Canada, les individus qui ont été victimes de violations à leur vie privée peuvent se prévaloir d'un nouveau délit en common law, soit « l'invasion de la vie privée ».

La plupart des pays font appel à un ensemble de lois pour couvrir l'étendue des questions relatives à la vie privée qui touchent leurs citoyens. Plus précisément, dans la plupart des réponses, on mentionne une combinaison de lois qui gouvernent deux grandes sphères de la vie privée : la protection des renseignements nominatifs d'une personne et l'accès à ces renseignements. D'une part, le cadre législatif relatif à la « protection de la vie privée » énonce comment les organismes gouvernementaux ou privés gèrent et traitent les renseignements personnels. D'autre part, le cadre législatif touchant à la « accès à l'information » permet généralement aux citoyens d'obtenir des renseignements sur les

dossiers d'intérêt public concernant les actions gouvernementales et de l'information détenue par les institutions gouvernementales sur une personne, un tel accès étant d'ailleurs matière à exceptions pour des motifs de sécurité nationale ou d'intérêt public.

La plupart des lois relatives à la protection de la vie privée abordées par les participants dans leur réponse semblent vouloir établir un équilibre entre le droit d'une personne à la protection de sa vie privée et les intérêts des autres à accéder, recueillir et publier des renseignements. Le consentement est très important dans les lois sur la protection de la vie privée, dans la mesure où il est souvent fondamental d'établir si la divulgation d'un renseignement précis entraînera une violation de la vie privée.

Dans certains pays comme l'Autriche et le Kazakhstan, le droit à la protection de la vie privée comprend le droit à l'« honneur ». En Autriche, les violations de ce droit comprennent tant « les violations de l'honneur comme telles » (par exemple les déclarations diffamatoires à l'égard du caractère ou du comportement d'une personne) que les violations en ce qui concerne les renseignements relatifs à la solvabilité d'une personne. En Tunisie, la protection des renseignements personnels liés à la vie privée d'une personne constitue un droit constitutionnel fondamental et doit être traité dans un contexte de transparence, de loyauté et de respect de la dignité humaine.

a. Dans le secteur public

*** L'accès des particuliers aux renseignements réunis sur eux par divers organismes gouvernementaux? * La protection de ces renseignements contre la divulgation à des tiers? * L'accès des membres des médias ou du public aux dossiers du gouvernement, par exemple, aux dossiers concernant la prise de décisions et de mesures gouvernementales, et les limites prévues?**

*** Les limites prévues en matière d'échange de renseignements entre organismes gouvernementaux?**

Pour ce qui est des renseignements détenus par les organismes gouvernementaux sur les personnes, le principe général semble être qu'il ne peut y avoir divulgation de tels renseignements personnels que si la personne visée y consent ou que la situation constitue une exception prévue. Ces exceptions concernent habituellement l'application de la loi et l'intérêt public.

Or, selon le principe général sous-jacent à l'« accès à l'information », une personne a le droit d'obtenir les renseignements recueillis à son sujet par les organismes publics, et on ne peut le lui refuser uniquement sur le motif que ces renseignements sont de nature personnelle. Toutefois, dans certains pays comme l'Irlande, Israël et la Suède, la loi sur la protection des renseignements personnels n'autorise pas l'accès aux renseignements sur la santé ou le travail social si la divulgation de ces renseignements est susceptible de nuire gravement à la santé physique ou mentale, au bien-être ou à la condition affective. Si on lui refuse l'accès aux renseignements, la personne peut demander qu'ils soient communiqués à un professionnel de la santé.

En outre, la plupart des pays reconnaissent, de façon assez générale, le droit d'accès du public et des médias à l'information sur les décisions et les actions gouvernementales. Cependant, la plupart des États

se réservent le droit de ne pas communiquer certains renseignements « à usage interne ». Par exemple, en Estonie, on compte parmi ces exceptions les renseignements recueillis lors d'instances criminelles, ceux recueillis lors d'instances de surveillance de l'état et ceux dont la divulgation nuirait aux relations internationales.

Échange de renseignements entre organismes gouvernementaux

L'échange de renseignement entre organismes gouvernementaux semble être assez limité dans la plupart des pays. Le principe général semble être que l'usage courant des renseignements doit être explicitement autorisé par la loi et les renseignements partagés ne doivent l'être que dans un but précis lié au mandat de l'organisme gouvernemental. À ce titre, le droit de partager des renseignements semble être assez rigoureusement contrôlé. Au Royaume-Uni, par exemple, le partage de données entre les différents organismes gouvernementaux est comparé au partage entre les personnes du secteur privé et les mêmes mécanismes de contrôle sont appliqués. Certains pays ont indiqué que le partage de renseignements entre organismes gouvernementaux était un peu plus vaste. Par exemple, en Australie, certains organismes gouvernementaux procèdent au recoupement des données, et ce, conformément à la législation. On peut définir le recoupement des données comme un regroupement de données provenant de différentes sources que l'on compare ensuite pour identifier des personnes en cas notamment d'action ou d'enquête pour un trop-perçu ou de fraude.

En Israël, la *Prohibition on Money Laundering Law* (loi sur l'interdiction du blanchiment d'argent) régit l'obtention de renseignements de la part de l'autorité chargée de l'imposition et des autorités policières; la loi sur la protection de la vie privée ne s'applique pas à la base de données créée conformément à cette loi. En outre, la *Biometric Identification and Data Law* (loi sur l'identification et les données biométriques) permet la création par le gouvernement d'une base de données d'identification biométrique (empreintes digitales et reconnaissance faciale) de la population israélienne, pour délivrer des pièces d'identité. Les fonctionnaires visés par cette loi sont habituellement en mesure de transmettre les renseignements, conformément à la loi, notamment aux autorités chargées d'appliquer la loi; dans d'autres cas, la transmission des données est limitée. Des inquiétudes ont été soulevées en Suisse à propos du « passeport biométrique » (c.-à.-d. un passeport contenant des renseignements comme des images du visage et des empreintes digitales enregistrées sur une puce électronique incorporée dans la couverture) introduit par le gouvernement fédéral. En effet, certains soutiennent qu'il n'existe pas de protection suffisante contre les agences douanières étrangères qui pourraient copier ou modifier les données personnelles stockées sur la puce.

b. Dans le secteur privé

- **La protection contre la divulgation à des tiers de renseignements personnels réunis dans le cadre du commerce électronique, par exemple :**
 - ✓ renseignements personnels fournis par le biais de cartes de crédit/de débit et autres transferts de fonds électroniques;
 - ✓ renseignements personnels obtenus aux fins d'évaluation du crédit et d'opérations bancaires;
 - ✓ dossiers sur les habitudes des usagers (téléphone; activités en ligne);
 - ✓ dossiers tenus aux fins de couverture d'assurance et autres prestations des services sociaux offertes par le secteur privé?

Dans certains pays, la protection des renseignements recueillis dans le cadre du commerce électronique est prévue par les principales lois en matière de protection de la vie privée. Dans d'autres pays, cette protection est couverte par des lois plus générales qui régissent les exigences en matière de transactions commerciales électroniques. Enfin, dans un plus petit nombre de pays, des lois précises visant la protection de la vie privée dans le cadre du commerce en ligne ont été adoptées. En Slovénie, le contenu des courriels est protégé directement par un article de la constitution slovène, dont les « données du trafic » du courriel (l'émetteur et le destinataire). En Géorgie, les communications par téléphone ou autres moyens techniques sont protégées par un article de la constitution géorgienne. En Lituanie, la *Electronic Communications Act* (loi sur les communications électroniques) régit l'utilisation des ressources, réseaux et services de communication électronique.

Dans certains cas, le « tiers » à qui on veut interdire la divulgation de renseignement peut être le gouvernement. Par exemple, les États-Unis ont adopté la *Electronic Communications Privacy Act* (loi sur la confidentialité des communications électroniques), laquelle interdit aux fournisseurs de communications électroniques de divulguer des renseignements de nature privée au gouvernement. Plus particulièrement, certains pays comme les États-Unis ont adopté des lois telles que la *Financial Privacy Act* (loi sur la protection des données financières), qui régit les questions relatives à la protection de la vie privée en ce qui a trait aux renseignements recueillis et conservés par les établissements financiers. Selon les dispositions de cette loi, les banques n'ont pas le droit de fournir de renseignements financiers personnels recueillis et conservés, sauf exception (si le client a donné son consentement, s'il y a un mandat de perquisition ou une citation à comparaître valide ou si le gouvernement présente une demande écrite officielle dans des circonstances particulières).

Certains pays ont décelé des problèmes permanents en matière de protection de la vie privée dans le cadre du commerce en ligne, entre autres le problème pratique de surveiller la conformité aux lois dans ce domaine. Par exemple, des pays ont souligné la difficulté à garantir la destruction totale des renseignements personnels conservés ou transmis par les grands organismes et le risque que les organismes passent outre ou ne fassent que des tentatives superficielles pour détruire les renseignements. Certains pays exigent que les organismes affichent des énoncés relatifs à la protection de la vie privée sur leur site Web, notamment sur la protection des données traitées sur le site Web, pour que les clients connaissent leurs droits en matière de protection de la vie privée pour ce site. Au Luxembourg, la loi interdit l'envoi de messages électroniques à des fins de sollicitation si l'identité de l'expéditeur est déguisée, cachée ou fausse ou si l'expéditeur n'a pas fourni une adresse valide à laquelle le destinataire peut envoyer une demande pour ne plus recevoir de messages de la sorte.

- **La protection contre la collecte clandestine de renseignements sur Internet, par exemple, au moyen de technologies de surveillance électronique telles qu'un « logiciel espion » ou un « logiciel de publicité »?**

La plupart des pays n'ont pas adopté de loi visant particulièrement les droits relatifs à la protection de la vie privée en ce qui concerne les technologies de surveillance sur Internet. Beaucoup de travail semble nécessaire sur la question du vol d'identité ou l'usage abusif de renseignements recueillis grâce aux technologies de surveillance sur Internet. Quelques pays se sont dotés de lois plutôt exhaustives contre la « surveillance secrète » ou la « surveillance électronique ». Aux États-Unis, il existe une loi qui criminalise la surveillance électronique et le vol de renseignements confidentiels, mais cette loi ne visait pas particulièrement les logiciels espions et de publicité au moment de son adoption. Il semble que dans les pays où il y a actuellement une forme ou une autre de loi de surveillance, les lois pertinentes devront vraisemblablement être révisées pour être adaptées aux nuances des technologies changeantes. On

peut trouver un exemple du type de problème qui émerge de la surveillance d'Internet dans la réponse de la Suisse. Dans ce pays, le commissaire sur les données a exigé que Google donne à toutes les personnes du pays qui apparaissent sur la fonction « Street View » de Google maps la possibilité, avant la publication, de choisir ou non s'ils voulaient que leurs données personnelles (image de la maison, de la voiture, adresse exacte) soient retirées ou non.

2. Quelles lois régissent les enquêtes et la protection des droits en matière de respect de la vie privée?

*** Cette protection est-elle suffisante? Les lois sont-elles exécutoires ou de nature informative? Comment un particulier peut-il porter plainte lorsqu'une entité privée ou un gouvernement enfreint les lois régissant le respect de la vie privée? Qui se charge de poursuivre ou de faire appliquer la loi – par exemple, un commissaire à la protection de la vie privée, un organe administratif, comme un tribunal de la vie privée? A-t-on prévu le droit à un recours judiciaire? A-t-on prévu des possibilités de règlement des litiges à l'amiable?**

La majorité des pays ont fait état d'un fort niveau de protection en matière de vie privée, à l'exception d'un petit nombre de pays. Ces derniers ont souligné, entre autres, les pouvoirs limités des commissaires à la protection de la vie privée et les lacunes des lois en cette matière comme facteurs diminuant les droits relatifs à la protection de la vie privée dans leurs pays. Plusieurs pays mentionnent le pouvoir limité de redressement du commissaire à la protection de la vie privée ou à l'information lui permettant de rendre des ordonnances exécutoires plutôt que faire de simples recommandations.

Les réponses des participants ont laissé entrevoir un éventail de régimes d'application. Les principales méthodes d'exécution comprenaient la poursuite en justice privée, l'action gouvernementale par l'intermédiaire d'un commissaire ou d'une autorité à la protection de la vie privée ou à l'information, l'autorégulation et la poursuite criminelle. Dans certains pays, il est possible d'interjeter appel des décisions administratives en matière de violation de la vie privée devant les tribunaux.

La plupart des lois en matière de protection de la vie privée sont contraignantes, mais les pouvoirs des commissaires à la protection de la vie privée ou à l'information varient substantiellement d'une réponse à l'autre des participants. Dans certains pays, le commissaire à la protection de la vie privée ou à l'information ne peut qu'enquêter et formuler des recommandations non contraignantes, tandis que dans nombre de pays, de tels commissaires peuvent entreprendre des actions en justice, rendre des décisions exécutoires et ordonner des mesures correctives. Par exemple, en Estonie, un organisme extrajudiciaire de protection des données peut intenter des poursuites si les droits d'une personne en matière de protection de la vie privée ont été violés. En Islande, l'Autorité pour la protection des renseignements personnels peut rendre légalement des décisions exécutoires sur toutes les questions touchant le traitement des données. En Pologne, un agent public spécial, l'inspecteur général pour la protection des renseignements personnels, peut intenter des procédures administratives et rendre des décisions exécutoires en ce qui concerne le traitement des renseignements personnels. En Italie, l'« Autorité garante pour la protection des données à caractère personnel » fonctionne de manière autonome et libre du contrôle ou de l'interférence des pouvoirs législatifs ou judiciaires.

Dans certains pays, l'accent est mis sur la correction des atteintes à la vie privée au niveau organisationnel. Le Japon a décrété que tout organisme qui enfreint la loi sur la protection de la vie privée doit volontairement corriger le manquement dans un premier temps; autrement, le ministre

compétent conseillera, recommandera ou ordonnera la correction du manquement. Le traitement des plaintes par une entreprise elle-même est perçu comme le moyen le plus important de traiter les violations à la vie privée afin d'accélérer la résolution des plaintes.

Les poursuites peuvent être entamées par des commissaires ou des autorités administratives dans le cadre de mesures administratives ou judiciaires. Les violations à la vie privée sont également poursuivies en justice criminelle dans certains pays dans le cas d'infractions comme la surveillance non autorisée d'Internet ou la communication non autorisée de renseignements relatifs à l'assurance maladie ou l'assurance vie. En Allemagne, l'utilisation de renseignements personnels, comme l'espionnage de fichiers informatiques enfreint les règlements du *Code criminel*. En Israël, certaines infractions pénales au droit à la vie privée donnent lieu à des dommages-intérêts automatiques fixés, sans qu'il faille prouver les dommages-intérêts réels. Au Portugal, l'accès non autorisé aux renseignements ou le non-respect des obligations relatives à la protection des données peut entraîner une peine maximale d'un an de prison. En ce qui concerne les enquêtes informatiques (logiciel espion), cette infraction peut entraîner une peine maximale de deux ans de prison. En vertu des lois relatives à la protection de la vie privée du Maroc, la collecte de renseignements personnels par des moyens frauduleux, sournois ou illicites est passible d'une peine d'emprisonnement de trois mois à un an.

Le vol d'identité est une autre infraction criminelle qui semble susciter de plus en plus d'attention, et quelques pays ont répondu à ce risque par l'adoption de lois plus larges visant à jeter un large filet sur des activités inappropriées. Par exemple, aux États-Unis, les autorités ne pouvaient autrefois que poursuivre une personne pour vol d'identité si cette personne avait utilisé les renseignements volés à quelques fins. En vertu de la nouvelle loi, la définition du vol d'identité comprend désormais le vol de renseignements en soi. En outre, même si la loi fédérale des États-Unis ne prévoit pas l'indemnisation des victimes de vol d'identité, certains États ont adopté une loi visant le dédommagement de ces victimes.

Peu de pays ont mentionné des solutions précises de règlement à l'amiable établies dans le but de résoudre les différends liés à la protection de la vie privée, à l'exception des modes substitutifs de règlement des conflits habituels (médiation, arbitrage, etc.). Dans certains cas, il est possible d'avoir recours à la conciliation par l'entremise du commissaire à la protection de la vie privée ou à l'information.

B. INITIATIVES DU SECTEUR PRIVÉ

- 1) Certaines entreprises, industries ou associations professionnelles de votre pays ont-elles leurs propres règles en matière de protection de la vie privée? Par exemple, existe-t-il des politiques, des codes professionnels, des normes volontaires en matière de respect de la vie privée?**

Le cadre législatif en matière de protection de la vie privée prévoit souvent l'obligation pour les entreprises privées de mettre en œuvre et de communiquer une politique organisationnelle en matière de protection de la vie privée. Une telle obligation comprend habituellement la nécessité d'élaborer une politique en matière de protection de la vie privée conforme aux lois pertinentes de l'État, d'aviser les

clients de l'existence de cette politique et de leur donner la possibilité de se retirer de tout programme de partage de renseignements.

En ce qui concerne les codes professionnels et les normes de l'industrie volontaires, les secteurs dans lesquels de tels codes ou normes semblent être assez communs dans de nombreux pays sont :

- les médias et le journalisme
- les télécommunications
- le marketing
- les soins de santé
- la biométrie
- les services bancaires et financiers
- les assurances
- les services juridiques

2) Qui ou quel organe, le cas échéant, s'assure que ces normes sont satisfaites?

Nombre des secteurs cités plus haut sont dotés d'associations d'autorégulation qui appliquent leurs propres codes et normes. La réponse des États-Unis laisse comprendre que l'autoréglementation par les organismes du secteur privé est en grande partie « dictée par les caprices du public ». Les normes volontaires en matière de respect de la vie privée découlent donc de la pression des consommateurs contre ce qu'ils jugent des atteintes inacceptables à leur vie privée.

Néanmoins, ces organismes doivent toujours se soumettre aux lois en vigueur en matière de respect de la vie privée dans leurs pays respectifs et demeurent subordonnés à l'autorité du commissaire à la protection de la vie privée ou à l'information compétent.

C. QUESTIONS INTERNATIONALES ET TRANSFRONTALIÈRES

1) Comment la vie privée est-elle protégée lorsque les renseignements sont échangés avec d'autres pays ou transmis à d'autres pays?

La principale méthode de protection de la vie privée en cas d'échange transfrontalier de renseignements semble être de limiter l'échange aux pays disposant d'un niveau de protection de la vie privée similaire afin d'éviter que les organismes n'enfreignent les obligations nationales en transmettant des renseignements à des pays ayant des normes moins élevées en matière de protection de la vie privée.

Dans certains cas, un organisme doit demander à l'autorité en matière de protection de la vie privée pertinente de son pays la permission de transmettre des renseignements si ces derniers sont envoyés dans un pays ne disposant pas d'un niveau suffisant de protection de la vie privée (selon l'opinion du pays transmetteur ou conformément à une convention pertinente).

2) Existe-t-il des ententes, lois, traités ou protocoles internationaux visant à protéger la vie privée dans ce cas?

D'après la directive relative à la protection des données de l'Union européenne (« UE »), il n'y a aucune restriction à l'échange de renseignements entre les pays membres de l'UE. En outre, selon la directive de l'Espace économique européen (EEE), il s'agit du territoire de l'UE plus la Norvège, l'Islande et le Liechtenstein), le transfert de renseignements peut se faire librement au sein de l'EEE. La Commission européenne est chargée de tirer des « conclusions » au sujet du caractère adéquat de la protection de la vie privée pour les pays qui ne font pas partie de l'UE.

L'UE a signé une entente « Safe Harbor » (Sphère de sécurité) avec les États-Unis, visant à créer une approche plus unifiée en matière de protection de la vie privée. En vertu de cette entente, les pays et les entreprises doivent respecter sept principes en matière de protection de la vie privée visant l'avis, le choix, le transfert à des tiers, la sécurité, l'intégrité des données, l'accès et l'application.

L'Australie et les États-Unis sont également signataires de l'entente de la Coopération économique Asie-Pacifique (APEC) visant l'application transfrontière des lois sur la protection des renseignements personnels, entente à caractère facultatif établissant un cadre pour l'application multilatérale des droits en matière de vie privée.

L'échange de renseignements fiscaux entre les autorités fiscales de différents pays est régi par des accords bilatéraux sur la double imposition. Certains pays ont adopté le *Modèle de convention concernant le revenu et la fortune* de l'Organisation de coopération et de développement économique (« Convention modèle de l'OCDE »). Conformément à la Convention modèle de l'OCDE, les pays doivent échanger des renseignements vraisemblablement pertinents à l'application correcte de la convention fiscale et à la gestion et l'application des lois fiscales des pays participants. En outre, dans le cadre de la Convention modèle de l'OCDE, les pays ne peuvent faire appel au secret bancaire pour refuser d'échanger des renseignements.

3) Votre pays limite-t-il l'échange de renseignements aux pays ayant les mêmes mesures de protection de la vie privée?

La majorité des pays ont affirmé que la transmission des renseignements se limite aux pays dont le niveau de protection de la vie privée est « adéquat » ou « suffisant ». Grâce à la directive précitée de l'UE et à la Convention n° 108 du Conseil de l'Europe, entre autres, il est facile d'établir ce niveau entre nombre de pays.

Beaucoup de pays ont signalé des exceptions courantes, des cas dans lesquels il serait acceptable de transmettre des renseignements à un pays dont le niveau de protection de la vie privée n'est pas jugé adéquat. Citons parmi ces exceptions :

- Si la personne concernée a expressément consenti à un échange de données précis;
- Si la personne concernée a rendu les renseignements accessibles publiquement et n'a pas expressément interdit leur transmission;
- Si l'échange des données est directement lié à l'exécution ou à l'achèvement d'un contrat et que les données visent une partie contractante;

- Si la transmission des données est essentielle à l'établissement, l'exercice ou l'application de recours devant les tribunaux;
- Si des règles internes assurent un niveau adéquat de protection (p. ex. si la divulgation est faite au sein de la même personne morale sous la même direction);
- S'il y a un intérêt public prépondérant à révéler les données à un pays étranger;
- Si la divulgation à un pays étranger est nécessaire pour protéger la vie ou l'intégrité de la personne concernée.

Toutefois, quelques pays ont rapporté ne pas limiter l'échange de renseignements aux pays disposant de mesures de protection de la vie privée similaires. En Australie, par exemple, il est de la responsabilité de chaque organisme d'évaluer le régime du pays dans lequel le partenaire commercial réside. Dans sa réponse, l'Australie a souligné que beaucoup de parties intéressées (surtout les petites entreprises) ont critiqué l'efficacité de ce système, affirmant ne pas détenir l'expertise et les ressources nécessaires pour juger des lois en matière de protection de la vie privée d'un pays étranger. Dans un même ordre d'idées, au Canada, les lois sur la protection des renseignements personnels obligent tous les organismes à utiliser des moyens contractuels ou autres pour offrir un niveau de protection comparable aux consommateurs quand les renseignements qu'ils ont en leur possession sont transmis à un tiers aux fins de traitement. Même si les lois canadiennes en matière de protection de la vie privée ne s'appliquent pas hors de leur territoire, les tribunaux ont soutenu qu'elles donnent néanmoins au commissaire à la protection de la vie privée le pouvoir d'enquêter sur les plaintes relatives à la circulation de l'information transfrontalière.