Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

16-Oct-2006

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

DSTI/ICCP/REG(2006)8/FINAL
Non classifié

Groupe de travail sur la sécurité de l'information et la vie privée

RAPPORT SUR L'APPLICATION TRANSFRONTIÈRE DE LA LÉGISLATION RELATIVE A LA VIE PRIVÉE

JT03215986

Français - Or. Anglais

AVANT-PROPOS

Plus de 25 ans après l'adoption des Lignes directrices de l'OCDE régissant la vie privée, pratiquement tous les pays de l'OCDE ont voté des lois sur la vie privée et ont donné le droit aux autorités d'imposer ces lois par la force. Toutefois, le volume et les caractéristiques des flux de données transfrontières ont évolué, élevant les risques liés à la vie privée, et augmentant les défis de l'application des lois transfrontières. Ce rapport décrit les tentatives actuelles pour s'occuper de ces défis et met l'accent sur le besoin d'une approche plus globale et méthodique pour une coopération pour la mise en application des lois transfrontières régissant la vie privée.

Le document a été préparé par le Secrétariat avec l'assistance des consultants Francis Aldhouse, Malcolm Crompton, et Peter Ford. Il a été révisé par un groupe de volontaires dirigé par Jennifer Stoddart, commissaire à la protection de la vie privée du Canada. Le Groupe de travail sur la sécurité de l'information et la vie privée a approuvé le document pour soumission au Comité de l'information, de l'informatique et des communications qui l'a déclassifié en octobre 2006.

Ce document est publié sous la responsabilité du Secrétaire Général de l'OCDE et est disponible en ligne à : www.oecd.org/sti/security-privacy.

POINTS SAILLANTS

La multiplication et la diversification des flux transfrontières de données accentuent les menaces sur la vie privée et rendent plus nécessaire une coopération renforcée pour l'application du droit.

Les évolutions observées dans les réseaux de communications mondiaux et les processus d'entreprises ont conduit à une augmentation des flux transfrontières de données. Les transferts de données dans des domaines tels que les ressources humaines, les services financiers, l'éducation, le commerce électronique et la recherche sanitaire – pour ne citer que ceux-ci – font dorénavant partie intégrante de l'économie mondialisée. Les progrès technologiques signifient que les données peuvent être transférées rapidement et stockées indéfiniment. Les transferts de données permettent une répartition mondiale des tâches qui tire avantage de l'expertise disponible en de multiples lieux à travers le globe, vingt-quatre heures sur vingt-quatre.

Les changements dans les flux de données internationaux, bien qu'ils aient apporté efficacité dans l'entreprise et commodité pour l'utilisateur, ont cependant entraîné une augmentation des risques pour la vie privée. Les transgresseurs cherchent à exploiter la technologie afin d'exposer des données parfois pour des raisons financières. En particulier, des cas récents de manquements à la protection des données ont notamment attiré l'attention, qui comportaient parfois une dimension transfrontière. Étant donné la facilité avec laquelle l'information peut être transférée instantanément, n'importe où, n'importe quand, l'aspect transfrontier des infractions à la protection des données risque d'augmenter. Comme avec le spam et la fraude transfrontière, la protection de la vie privée dans un environnement mondial dépend de la co-opération transfrontière. Bien que le besoin d'une véritable coopération en matière d'exécution ait été signalé depuis de nombreuses années, on note désormais un regain d'intérêt pour une action au niveau international destinée à remédier aux problèmes que pose l'application efficace des législations dans un monde où les flux de données internationaux sont généralisés et continus.

Les autorités chargées de la protection de la vie privée sont maintenant largement répandues dans les pays de l'OCDE. Elles partagent une identité de pouvoirs et de compétences.

Lorsque les Lignes directrices de l'OCDE sur la vie privée ont été adoptées il y a plus de 25 ans, seul un tiers environ des pays membres disposait d'une législation en matière de respect de la vie privée. Aujourd'hui la quasi-totalité des membres de l'OCDE sont dotés de législations – qui suivent pour la plupart les principes établis dans les Lignes directrices de l'OCDE sur la vie privée – et ont créé des organismes chargés de veiller à leur application.

Même si les autorités des pays membres partagent des points communs au niveau des pouvoirs qui leurs sont attribués et des lois qu'elles font respecter, des différences demeurent. Certaines autorités sont chargées de résoudre les plaintes individuelles, d'autres de superviser la conformité avec la réglementation et beaucoup assument ces deux tâches à la fois. Des différences existent en ce qui concerne les processus de traitement des plaintes, les pouvoirs d'enquête ou de vérification et les sanctions et moyens de réparation disponibles en cas d'infraction. Certaines autorités sont indépendantes alors que d'autres sont installées au sein de ministères ou de services gouvernementaux. Certaines couvrent la sphère publique, d'autres uniquement le secteur privé et beaucoup couvrent les deux domaines. Quelques rares autorités ont

pour mandat d'appliquer les textes protégeant la vie privée dans un secteur économique déterminé, par exemple, les télécommunications ou les services financiers.

Les autorités protégeant le respect de la vie privée rencontrent des difficultés dans le contexte des situations transfrontières.

Bien que presque toutes ces autorités puissent agir contre le responsable dans le pays d'un traitement de données au profit d'un étranger, les pouvoirs de beaucoup d'entre elles sont limités pour ce qui est de la protection de leurs propres résidents contre des violations de leur vie privée par le responsable étranger d'un traitement de données. Certains sont concernés par leur capacité juridique à prendre part aux activités d'applications. Certaines trouveraient avantageux de disposer de pouvoirs élargis pour échanger des informations et pour mener des investigations en commun ou à la demande d'une autorité étrangère. Enfin, dans un contexte transfrontière, les efforts des autorités sont parfois limités par des pouvoirs insuffisants, l'incompatibilité des régimes juridiques, un manque de ressources et d'autres obstacles pratiques.

Il existe déjà un certain nombre d'instruments régionaux et d'autres mécanismes moins formels destinés à faciliter la coopération transfrontière, mais aucun n'a une portée mondiale.

Les travaux du Conseil de l'Europe, de l'Union européenne et de l'APEC ont contribué à l'établissement d'un cadre pour une coopération entre les autorités d'application à l'échelle régionale. Ils ont ainsi débouché sur le développement récent de l'audit conjoint en Europe. Des contacts et des échanges d'informations plus informels ont lieu lors de la Conférence internationale des commissaires à la protection des données et à la vie privée, du Forum des autorités de protection de la vie privée d'Asie-Pacifique, au Groupe de travail international sur le protection des données dans les télécommunications et dans le cadre du Réseau ibéro américain de protection des données. Une coopération entre autorités chargées de la protection de la vie privée est également possible dans le cadre des recommandations de l'OCDE récemment adoptées sur la coopération en matière d'application de la législation anti-spam.

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.

Le respect de la vie privée est un domaine dans lequel les perceptions et les craintes du public peuvent évoluer rapidement. Le double objectif des Lignes directrices de l'OCDE de 1980 – à savoir protéger la vie privée et les libertés individuelles tout en évitant la création d'obstacles inutiles aux flux transfrontières de données à caractère personnel – demeure toujours pertinent aujourd'hui et il l'est peut-être même davantage avec la progression des volumes de données qui franchissent les frontières. Il est important pour le maintien de cet équilibre de mettre en place un cadre permettant de mener des actions de coopération pour répondre aux problèmes lorsqu'ils se présentent. En outre, une plus grande transparence dans le fonctionnement de la protection de la vie privée contribuerait à son respect par les entreprises et renforcerait la confiance des utilisateurs dans la protection de la vie privée au niveau mondial. L'objectif fondamental de tout effort d'amélioration de la coopération en matière de protection devrait être la protection de l'information à caractère personnel des individus, où qu'elle soit.

TABLE DES MATIÈRES

INTRODUCTION : FLUX TRANSFRONTIÈRES DE DONNÉES, RISQUES POUR LA VIE PRIVÉE ET COOPÉRATION EN MATIÈRE D'APPLICATION

Le défi que représente la protection de l'information à caractère personnel lorsqu'elle franchit les frontières est maintenant bien connu. Les premiers efforts entrepris pour prendre en compte la protection de la vie privée au niveau international remontent à la fin des années 1970 quand l'OCDE et le Conseil de l'Europe ont lancé leurs travaux de référence dans le domaine. Alors que beaucoup a été fait au cours des années qui ont suivi pour améliorer la protection de la vie privée à travers le globe, l'essor d'Internet et les changements qu'il a entraîné en ce qui concerne le volume et les caractéristiques des flux mondialisés de données à caractère personnel ont accru les risques pour la vie privée. Cette évolution fait ressortir le besoin d'une coopération mondiale plus structurée pour assurer la protection de la vie privée.

Le présent rapport fait le point sur les autorités chargées de l'application de la législation et sur les mécanismes qui ont été mis en place pour protéger la vie privée, en s'intéressant particulièrement à leur mode de fonctionnement dans le contexte transfrontière. Il décrit les défis actuels rencontrés pour une application efficace ainsi que les mécanismes existants pour y remédier. Il s'achève par une série de questions dont il conviendrait d'approfondir l'analyse, afin d'aider ceux qui sont chargés de faire appliquer la législation sur la protection de la vie privée à protéger les informations à caractère personnel où qu'elles se trouvent.

A. Cadres internationaux de protection de la vie privée

Les Lignes directrices de l'OCDE sur la vie privée visaient à répondre aux préoccupations suscitées par l'opposition entre législations nationales en matière de protection des données. Parmi ces buts il y avait le souci de faire en sorte que la multiplication des législations nationales de protection des données ne bloque pas les flux transfrontières de données au détriment de la croissance économique. Dans le même temps, les Lignes directrices ont fait ressortir que les pays de l'OCDE avaient un intérêt commun en matière de protection de la vie privée et des libertés individuelles. Face à la double préoccupation suscitée d'un côté par les menaces envers la vie privée du fait d'un usage plus intensif des données à caractère personnel et de l'autre par le risque pour l'économie mondiale de restrictions sur les flux d'information, l'OCDE a élaboré ce qui a fini par être reconnu comme l'une des affirmations majeures des principes fondamentaux de la protection de la vie privée.

L'adoption des Lignes directrices de l'OCDE sur la vie privée en 1980[1] a représenté un pas significatif dans le processus de protection internationale de la vie privée. La Convention du Conseil de l'Europe de 1981[2] (" Convention 108 ") et par la suite la Directive de l'Union européenne 95/46/EC (la Directive de l'UE) ont marqué de nouvelles avancées dans l'élaboration des politiques et législations en matière de protection de la vie privée. En particulier, la Directive de l'UE a défini des règles visant à faire en sorte que les normes en matière de protection de la vie privée appliquées au sein de l'Europe ne soient pas affaiblies par le transfert de données entre l'Europe et d'autres pays. En 1990, l'Assemblée générale des Nations Unies a adoptée des Principes directeurs qui reflètent ceux énoncés dans les Lignes directrices de l'OCDE et la Convention 108, tout en mettant d'avantage l'accent sur les droits de l'homme.[3] Plus récemment les économies du Forum de coopération économique Asie-Pacifique (APEC) ont finalisé un ensemble de mesures appelé Cadre de l'APEC sur la vie privée. Celui-ci propose une approche centrée sur la prévention des préjudices résultant d'une utilisation abusive de l'information à caractère personnel ainsi

qu'un principe de responsabilité lorsque les données franchissent les frontières. Ce Cadre a été approuvé par les ministres de l'APEC en 2004.[4]

B. Économies ouvertes et réseaux de communications

Changements dans les flux d'information mondiaux

L'innovation technique permanente et l'évolution sociétale au sein d'Internet ont modifié le paysage des communications et des flux d'information mondiaux. Lorsque les Lignes directrices de l'OCDE ont été adoptées en 1980, les flux transfrontières de données à caractère personnel pouvaient être considérés comme des évènements isolés dans lesquels des données étaient transférées en grande quantité entre des parties identifiées. On observait ainsi des transferts de lots importants de données sur des supports physiques tels que des bandes magnétiques. Les banques de données internationales venaient d'apparaître et l'Internet n'en était encore que dans ses toutes premières phases, qui excluaient les usages commerciaux.

Il est difficile d'obtenir des estimations précises du volume d'informations qui franchissent aujourd'hui les frontières, mais les données connexes sont instructives. Le nombre global d'utilisateurs d'Internet approche maintenant le milliard et la part des abonnements à large bande a quadruplé entre 2001 et 2005.[5] Les capacités de trafic international d'Internet continuent à croître et par exemple la capacité des nœuds d'interconnexion de San Francisco ou Tokyo a plus que doublé entre 2002 et 2003 et à nouveau quasiment doublé en 2004.[6] De même les coûts du transit international ont chuté de manière importante. Certains estiment que ce qui aurait coûté USD 1 000 par Mbps par mois en 1995 ne coûtait plus que 15 USD par Mbps par mois en 2005.[7] Bien que ne constituant pas une mesure directe du volume des flux transfrontières de données, ces chiffres permettent de donner une illustration d'un monde interconnecté dans lequel les flux d'information sont fluides et décentralisés et dans lequel les échanges transfrontières de données se sont banalisés. Désormais un même « clic » de souris permet de transférer des données de l'autre coté du globe ou de l'autre coté du couloir.

Cette caractéristique principale de l'environnement actuel a été soulignée par de nombreux observateurs. L'information « circule plus librement, connaît moins d'entraves nationales et de fait représente l'une des forces majeures qui participent au processus de mondialisation ».[8] L'information « est devenue la nouvelle matière première de l'économie mondiale ».[9] Ou, suivant la documentation sur les principes des Accords de la sphère de sécurité entre les Etats-Unis et l'UE, les transferts de données sont la ressource vitale de nombreuses organisations et la base de tout le commerce électronique. Les organisations multinationales partagent communément entre leurs différents sites un somme considérable d'informations à caractère personnel. »[10] Ainsi de plus en plus d'entreprises, de gouvernements et d'activités individuelles migrent vers les réseaux mondiaux IP à connexion permanente. Les échanges transfrontières de données à caractère personnel ont toutes sortes de motifs : commerce électronique, administration électronique, banque en ligne, gestion des ressources humaines, enseignement à distance, jeux en ligne, activités communautaires ou associatives ou recherche médicale – pour n'en citer que quelques-unes.

Des individus se connectent couramment avec d'autres partout dans le monde, échangent des profils et des préférences, tiennent des blogs, expriment des avis sur de la musique, ou font des achats sur des sites d'enchères en ligne[11] Ils effectuent des achats et des réservations de voyages auprès d'entreprises étrangères via Internet. Des réseaux financiers et des services de messagerie sophistiqués facilitent l'utilisation des cartes de crédit et de débit à travers le monde. Les multinationales transfèrent les informations à caractère personnel sur leurs clients et les dossiers de leurs employés à travers les frontières. Les gouvernements proposent de plus en plus de services par voie électronique pour améliorer leur fonctionnement interne et offrir de meilleures prestations au secteur privé et aux citoyens. Ils échangent

également entre eux des informations à caractère personnel pour diverses raisons telles que le contrôle aux frontières.

Les organisations ont modernisé leurs opérations en en organisant la gestion à partir des sites les plus rentables. De nombreux agents différents peuvent participer à la collecte et au transfert des données, que ce soit au nom de la société ou pour le compte d'un tiers. Des fonctions précédemment centralisées comme le traitement des paiements, la vérification de crédit, le service client, ou l'assistance technique peuvent être disséminées dans le monde pour tirer avantage des compétences sur différents sites. Il est fréquent de voir confier à des sites offshore le traitement externalisé des transactions par cartes de crédit, de la facturation téléphonique et des dossiers médicaux dans le but de tirer profit de coûts moins élevés et de la spécialisation des compétences. De nombreuses entreprises ont établi des centres de service client à l'étranger pour répondre aux attentes de leur clientèle qui exige une assistance en temps réel. Pour permettre de répondre aux demandes 24 heures sur 24, sept jours par semaine, les données devront sans doute être transférées vers des sites où ces horaires correspondent aux horaires de travail normaux du personnel d'assistance selon le modèle de délocalisation dit « suivre le soleil ».

Le câble, les télécommunications et les réseaux mobiles vont dans l'avenir converger vers le protocole Internet (IP) et les réseaux de nouvelle génération (NGN) pour permettre le transport de la voix, de la vidéo et des données sur la même infrastructure. Le déploiement des réseaux de puces RFID et de capteurs va prochainement entraîner une généralisation encore plus grande des canaux de communication et accentuer davantage la croissance exponentielle des flux ininterrompus de données.[12]

Évolution des risques pour la vie privée

La croissance des réseaux de communication et d'information, en taille, en sophistication et en fonctionnalités permet une plus large efficacité pour les entreprises et un plus grand confort pour les utilisateurs mais elle s'accompagne également d'une modification des risques portant sur les données privées des individus et des organisations. Le premier tient par définition à l'expansion des flux transfrontières de données. En effet, la multiplication des flux transfrontières de données, à des débits plus élevés, couvrant des zones géographiques plus étendues, et englobant des données alphanumériques, de la voix et des images entre une multiplicité croissante d'acteurs est susceptible d'augmenter le nombre et le coût des violations de la vie privée subies par les individus et les organisations. Ce changement d'échelle pourrait, si un « point d'inflexion »[13] était atteint, conduire à une perte de confiance des utilisateurs et en conséquence à un changement des comportements.[14] Selon un sondage réalisé auprès de consommateurs dans 12 pays pour le compte de la société VISA, dans une liste de maux comprenant la maladie, les catastrophes naturelles, le terrorisme, la protection de l'environnement et la perte d'emploi, la question qui préoccupait le plus les individus était la perte ou le vol des informations à caractère personnel ou financières.[15] Même si souvent, la constatation des craintes des consommateurs ne semble pas s'accompagner d'un changement des comportements, il ne faut pas sous-estimer le risque que des violations répétées de la vie privée mettent en péril les efforts entrepris pour renforcer la confiance dans les transactions en ligne et empêchent la poursuite de l'expansion de l'économie numérique. Certaines études suggèrent déjà que l'intérêt des consommateurs pour les transactions bancaires en ligne serait peut-être en train de diminuer en raison des inquiétudes sur le détournement des informations à caractère personnel,[16] et que s'ils ont connaissance d'une violation de la sécurité, de nombreux consommateurs vont décider de changer d'institution.[17]

Plus spécifiquement, et au-delà du risque d'échelle, deux catégories de risques pour la vie privée semblent prévaloir, résultant tous deux de l'évolution de l'environnement technologique : *i)* les risques relatifs aux utilisations secondaires des données à caractère personnel et *ii)* les risques relatifs aux violations de la sécurité de l'information. Pour ce qui est de l'utilisation secondaire, les particuliers ont toujours eu du mal à surveiller la façon dont les organisations utilisent leurs données, mais la facilité et la

fréquence avec laquelle les organisations traitent les données aujourd'hui exacerbent le problème. Comme le professeur Peter Swire l'a récemment souligné, nous sommes maintenant dans un environnement où des quantités sans précédent d'informations à caractère personnel font l'objet de transfert instantané entre ordinateurs. Si les consommateurs ne peuvent pas contrôler efficacement la vente de leurs données, les entreprises vont être incitées à « sur-utiliser » les données à caractère personnel en les revendant contre rémunération.[18] En mars 2006, une action a été engagée contre une société Internet basée aux États-Unis ayant vendu des informations à caractère personnel collectées auprès de millions d'individus en dépit d'une promesse de confidentialité figurant dans la charte de protection de la vie privée du site Internet de la société.[19]

Autre élément attestant d'une augmentation des risques, un nombre croissant de violations de la sécurité des données sont rendues publiques. Au Japon, le Cabinet du Premier ministre a signalé que le nombre de cas de violations d'informations personnelles publiquement annoncé par les organisations avait dépassé 1 500 en 2005.[20] Il est indéniable que le public accorde une attention croissante à ces violations, en partie grâce à une augmentation de déclarations obligatoires de lois.[21] Bien que les incidents de violations de la sécurité des données n'entraînent pas toujours des pertes financières pour les individus, certains causent des dommages significatifs. L'une des plus grosses affaires signalées concernait une société de traitement de paiement par carte basée aux États-Unis, *CardSystems Solutions*. Cette société a conclu un arrangement avec la *Federal Trade Commission* (FTC) qui l'accusait de ne pas avoir pris les mesures de sécurité appropriées pour protéger les données sensibles de dizaines de millions de consommateurs, ce qui avait entraîné des millions de dollars d'achats frauduleux.[22] Ce manquement à la sécurité a eu des répercussions dans d'autres pays et en particulier au Japon où des dizaines de milliers de cartes ont été compromises par la défaillance du *CardSystems*, ce qui a entraîné une perte estimée à JPY 110 millions.[23] L'affaire *CardSystems* a suivi de près un manquement à la sécurité chez le courtier de données de consommateurs *ChoicePoint,* qui s'est traduit par la compromission des dossiers financiers personnels de plus de 163 000 individus et au moins 800 cas d'usurpation d'identité.[24] La "*Privacy rights Clearinghouse*" tient une liste détaillée des manquements à la sécurité des données, et elle estime que près de 90 millions de dossiers ont été compromis depuis l'incident *ChoicePoint*.[25] Cependant, du fait qu'en général les organisations ne jugent pas productif de rendre publiques les violations de sécurité, l'ampleur du problème n'est peut-être pas entièrement connue.[26]

S'il est probable qu'un certain nombre de violations de la sécurité des données ont un impact au-delà des frontières du pays dans lequel elles sont signalées, l'aspect transfrontière n'est pas souvent pris en compte par les autorités ou par la presse. Or de nombreux incidents de violations transfrontières ont été portés à la connaissance du public. Ainsi, une société canadienne a récemment annoncé avoir perdu un ordinateur contenant les noms et numéros de sécurité sociale de 1.3 million d'étudiants américains.[27] D'autres affaires sont liées à l'externalisation offshore. En 2005, les médias ont indiqué que l'identité des clients pouvait être aisément achetée auprès des centres d'appels exploités en Inde pour les banques anglaises.[28] En juin 2006 des articles ont signalé au Royaume-Uni des violations transfrontières portant sur les données de 2 500 employés américains,[29] et en Inde la police a arrêté un employé d'un centre de services client d'une institution financière internationale ayant accédé illégalement aux informations des comptes de clients du Royaume-Uni et ayant occasionné le détournement de GBP 200 000.[30] Les pirates informatiques sont également susceptibles de commettre des violations. En juillet 2006, un pirate informatique situé en Allemagne a obtenu l'accès au système informatique d'une agence gouvernementale locale aux États-Unis qui contenait des informations à caractère personnel sur 4800 résidents de HLM. [31] Il existe aussi d'autres risques transfrontières, comme le fait que la divulgation par inadvertance de données à caractère personnel sur un site Internet public puisse être la cause d'un usage inapproprié dans n'importe quel pays autour du globe. [32]

Les autorités chargées de la protection des données et de la vie privée ne déclarent recevoir qu'un nombre limité de plaintes transfrontières. Il est en effet certain que peu de plaintes individuelles comportent un élément transfrontière, à l'exception notable des spams. Bien que cela puisse suggérer qu'il y ait peu de violations de la vie privée comportant une dimension transfrontière, cela peut tout aussi bien indiquer un manque d'information de qualité sur le sujet. Un examen plus approfondi des tendances des plaintes pourrait être donné à titre indicatif. Par exemple la proportion des plaintes des consommateurs concernant des fraudes de la base de données conjointe États-Unis-Canada-Australie « *Consumer Sentinel* » indique que la proportion de plaintes pour fraude ayant un caractère transfrontière est en augmentation constante : 20% des plaintes avaient un caractère transfrontière en 2005, contre 16% en 2004 et 14% en 2003. [33]

Il est difficile de déterminer si les plaintes pour atteinte à la vie privée vont suivre la tendance plus générale des plaintes pour fraude à la consommation. Tout d'abord les individus peuvent ne pas être au courant de l'utilisation de leurs données à caractère personnel à l'extérieur des frontières de leur pays. Dans certains cas, les victimes peuvent même ne pas avoir conscience que leurs plaintes impliquent une organisation étrangère. Les victimes peuvent ne pas savoir à qui s'adresser dans le cas d'un problème transfrontière. En fait, même dans le cas d'un problème purement national, les victimes peuvent ignorer à qui s'adresser pour présenter leurs plaintes. En Norvège, une étude récente a mis en lumière que seuls 33% des Norvégiens savaient que l'Inspection des Données était l'autorité chargée de la protection des données à caractère personnel[34], tandis que seul 15% du public du Royaume-Uni avait connaissance du rôle de l'Office du commissaire à l'information (*Information Commissioner's Office*). [35]Au total, les enquêtes sur les attitudes du public suggèrent que seul un pourcentage très réduit d'individus allait s'adresser à l'autorité de protection de la vie privée compétente.[36] Des récents efforts afin d'améliorer la rédaction des notices de protection de la vie privée par les organisations qui traitent des données pourraient à certains égards aider les particuliers sur l'exercice de leurs droits au respect de la vie privée. [37]

Davantage de recherches, d'informations et d'analyses aideraient à se faire une image plus claire de la nature des risques pour la vie privée découlant de l'évolution de l'environnement des flux transfrontières de données. Mais il est déjà évident que ces risques qui ont causés des dommages aux particuliers et aux organisations et menacent également le climat de confiance nécessaire à l'endroit d'une économie mondialisée fondée sur la circulation libre de l'information.

C. L'initiative actuelle de l'OCDE

Les Lignes directrices de l'OCDE sont non seulement un énoncé de principes sur l'utilisation des informations à caractère personnel mais aussi un appel à des initiatives de mise en œuvre sur le plan national (Partie IV) et à une coopération internationale en vue de faciliter les flux transfrontières de données personnelles respectant les principes de protection contenus dans les Lignes directrices (Partie V). La Partie V prévoit notamment que :

> « Les pays membres devraient établir des procédures en vue de faciliter l'échange d'informations relatives aux présentes Lignes directrices ; et l'assistance mutuelle lorsqu'il s'agit des questions de procédures et d'échange réciproque d'information. »

L'OCDE a continué de bâtir sur le socle établi par les Lignes directrices, notamment dans le domaine du commerce électronique. Lors de leur réunion d'Ottawa en 1998, les ministres de l'OCDE ont déclaré :

> « Qu'ils prendront, dans le cadre de leurs lois et pratiques respectives, les mesures nécessaires pour garantir la mise en oeuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée en ce qui concerne les réseaux mondiaux, en veillant notamment : …à garantir l'existence de mécanismes efficaces de mise en oeuvre permettant à la fois de régler les problèmes de non-respect des principes et des politiques de vie privée et de garantir l'accès à des moyens de réparation ». [38]

L'importance d'une mise en application efficace a de nouveau été soulignée dans le rapport de l'OCDE de 2003 intitulé « Protection de la vie privée en ligne: orientations politiques et pratiques de l'OCDE » qui appelait les pays membres à « s'efforcer d'établir des procédures pour améliorer les mécanismes bilatéraux et multilatéraux de coopération transfrontière entre les organismes publics chargés de l'application de la loi et concernés par les aspects de procédure ou d'investigations associés aux Lignes directrices ou prévus par elles. » [39]

Au cours des dernières années, l'OCDE a abordé d'autres aspects du commerce électronique mondial pouvant présenter des menaces contre les individus et ainsi réduire la confiance dans les transactions en ligne. Elle a travaillé en particulier pour combattre le phénomène des courriers électroniques non sollicités (spam)[40], et a pris des mesures pour encourager et faciliter la coopération entre les autorités chargées de la protection des consommateurs en vue de prévenir les opérations frauduleuses contre ces derniers. [41]Ces deux initiatives reflètent la nécessité de renforcer la coopération internationale en matière d'application de la loi et fournissent une illustration du rôle que peut jouer l'OCDE dans la facilitation d'une telle coopération.

Dans ce contexte, le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée (GTSIVP) a entrepris l'examen des questions soulevées par l'application transfrontière des lois sur la protection de la vie privée. L'objectif est d'étudier la question tant du point de vue des pays membres que des pays non membres de l'OCDE. Les actions formelles de mise en application sont habituellement considérées comme le denier ressort parmi la large gamme des mécanismes destinés à assurer une mise en oeuvre effective de la législation. Les travaux antérieurs de l'OCDE ont reconnu l'importance des incitations faisant appel au marché, des outils techniques (par exemple les technologies protectrices de la vie privée TPVP), des garanties de tierces parties (par exemple marques de confiance ou labels) et des structures organisationnelles (par exemple *chief privacy officers*). [42]Mais il faut parfois imposer le respect de la législation et ce projet vise à contribuer à la solution aux problèmes rencontrés à cet égard dans un environnement transfrontière.

A titre de première étape, le GTSIVP a élaboré un questionnaire à l'intention des pays membres dans le but de comprendre l'environnement actuel de la coopération entre les autorités d'application. La participation de pays non membres a également été recherchée pour le recueil des réponses au questionnaire afin de disposer d'une image plus complète de la situation à travers le globe. Le questionnaire visait à obtenir suffisamment d'information sur les autorités de mise en œuvre de la protection de la vie privée dans le but : *i)* de comprendre le contexte juridique dans lequel évoluent ces autorités, *ii)* d'identifier les défis actuels que pose la coopération transfrontière et *iii)* d'indiquer des pistes prometteuses pour faire face à ces défis. Ce projet est centré sur les efforts déployés par les organismes gouvernementaux pour faire appliquer la législation ou les réglementations relatives à la vie privée régissant tant le secteur public que le secteur privé. Il ne couvre pas, par exemple, les initiatives de la région Asie Pacifique relatives à la mise en application de la législation par des organisations non gouvernementales ou qui mettent en jeu des principes de protection de la vie privée différents de ceux qui sont sanctionnés dans la législation étatique.

Le reste de ce rapport est composé de deux sections principales et d'une conclusion. La première section du rapport offre une vue d'ensemble des mécanismes de base de mise en œuvre de la protection de la vie privée dans le contexte national. La seconde section traite des aspects transfrontières de la mise en œuvre de la protection de la vie privée, en s'intéressant aux problèmes particuliers rencontrés par les autorités ainsi qu'aux solutions actuellement adoptées pour y faire face. Ce rapport comprend également une section consacrée aux travaux récents de l'OCDE dans deux domaines connexes : les spam et la protection des consommateurs. La conclusion expose l'analyse qui ressort de ce projet ainsi qu'une liste de thèmes pouvant faire l'objet d'études ultérieures.

SECTION I. ASPECTS NATIONAUX DE L'APPLICATION DE LA LÉGISLATION POUR LA PROTECTION DE LA VIE PRIVÉE

Le questionnaire d'enquête a été distribué en février de 2006. A la mi-juin, 21 pays membres avaient répondu : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la France, la Hongrie, l'Islande, l'Italie, le Japon, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, la République tchèque, le Royaume-Uni, et la Suisse. En outre, une économie non membre, l'Albanie, a envoyé une réponse bienvenue. Un tableau récapitulatif des réponses est joint en annexe A. De plus, une brève introduction à la législation sur la protection de la vie privée dans les pays non membres de l'OCDE est jointe en annexe B à titre de référence.

Le questionnaire mettait l'accent sur la mise en application (exécution) de la législation relative à la vie privée par les autorités gouvernementales. Le questionnaire définissait le terme exécution comme désignant les efforts des autorités gouvernementales pour *i*) assurer des recours juridiques aux particuliers qui ont subi un préjudice ; *ii*) procéder à des contrôle du respect des réglementations et à des inspections ; et *iii*) assurer le respect des législations par des actions juridiques officielles à caractère administratif, civil ou pénal. La présente section du rapport tente de décrire les mécanismes d'exécution mis en lumière par les réponses au questionnaire, avec l'aide sur certains points de sources additionnelles. Le tableau des réponses joint en annexe comprend des doubles réponses pour la Corée et les Pays-bas ainsi qu'une réponse limitée au secteur privé pour le Japon. Il n'y a qu'une seule réponse pour l'Allemagne décrivant la fonction du Commissaire fédéral mais l'Allemagne a fourni une réponse très complète exposant sa structure complexe d'application de la législation fédérale et locale, dont le texte suivant tente de rendre compte.

Compte tenu de la composition de l'OCDE, la majorité des répondants est membre de l'Union européenne ou de l'Espace économique européen (EEE) ainsi que du Conseil de l'Europe. Ceux-ci sont en conséquence liés à la fois par la Convention 108 et la Directive européenne 95/46/CE. En conséquence, les réponses de ces pays présentent de grandes similitudes. Dans leur ensemble, toutefois, les réponses témoignent également d'une grande diversité au sein des différentes autorités chargées de l'application, que le présent rapport décrit en partie. Il n'est pas certain, cependant, que cette diversité crée un obstacle en pratique à la coopération en matière d'application.

A. Mécanismes de base en matière d'application

Les autorités et leur champ de compétence

Le questionnaire demandait aux pays de mettre l'accent sur les autorités d'application au niveau national. Certaines réponses ont apportées des informations supplémentaires à l'explication de la complexité de leurs mécanismes nationaux soit par leur structure fédérale soit par d'autres raisons telles que la multiplicité des lois ayant une incidence sur la vie privée ou l'existence de mécanismes d'application différents dans les secteurs public et privé. Par exemple en raison de la structure fédérale de l'Allemagne, le respect des dispositions sur la protection des données régissant les secteurs public et privé est principalement assuré par des autorités régionales indépendantes.

L'impression générale qui se dégage des réponses est qu'il existe bien dans les pays membres des autorités chargées au niveau national de l'application de la législation sur la protection de la vie privée bien que dans certains pays, comme aux États-Unis, ces fonctions puissent être considérées comme faisant principalement partie de la mise en oeuvre de la protection des consommateurs. Dans la majorité des cas, en raison de l'appartenance à l'Union européenne, les autorités ont été mises en place dans le cadre de législation générale de transposition de la Directive européenne dans le but de contrôler les secteurs public et privé au moyen de pouvoirs identiques. Cette image de l'Union européenne est néanmoins brouillée par l'Allemagne, qui fut l'un des premiers pays à adopter une législation de protection des données, car suivant sa structure fédérale, l'application en ce qui concerne le secteur privé est principalement de la compétence des régions. Habituellement une autorité d'application est constituée d'un commissaire unique, indépendant du gouvernement, chargé d'étudier les plaintes des particuliers et de superviser les activités de traitement des données des responsables de traitements des données. Toutefois, certains pays ont choisi de créer des commissions composées d'un ensemble de commissaires, par exemple la France, la Belgique et les États-Unis. Ces commissions peuvent être compter un plus ou moins grand nombre de personnes et siéger à temps plein ou à mi temps. Pour un second groupe de pays dont le Japon, la Corée et certains des états allemands, des groupes de fonctionnaires appartenant aux différents ministères sont chargés de veiller à la protection de la vie privée. Il n'est donc pas surprenant de constater que même si la Directive de l'Union européenne impose un certain degré d'uniformité, la structure des autorités d'application est très variée.

Le tableau suivant donne la liste des autorités d'application de la protection de la vie privée au niveau national pour les pays de l'OCDE et les liens vers des sources d'information à leur sujet. Il faut garder à l'esprit que les pays à structure fédérale comme l'Allemagne, l'Australie, le Canada et les États-Unis sont dotés d'autorités d'application régionales qui jouent souvent un rôle important dans l'application de la protection de la vie privée et donc la liste ci-dessous n'offre qu'une image incomplète.

Tableau 1. Autorités d'application pour la protection de la vie privée au niveau national dans les pays de l'OCDE

Allemagne	Commissariat fédéral pour la protection des données et la liberté de l'information	www.bfdi.bund.de
Australie	Privacy Commissioner	http://www.privacy.gov.au
Autriche	Datenschutzkommission	http://www.dsk.gv.at
Belgique	Commission de la Vie Privée	http://www.privacycommission.be
Canada	Commissariat à la protection de la vie privée du Canada	www.privcom.gc.ca
Corée	Ministère de l'Information et de la Communication	www.mic.go.kr
	Agence coréenne de sécurité de l'Information	www.kisa.or.kr
Danemark	Datatilsynet	www.datatilsynet.dk
Espagne	Autorité espagnole de protection des données	www.agpd.es
États-Unis	Federal Trade Commission	www.ftc.gov
	Department of Heath and Human Services	www.hhs.gov
	Federal banking agencies	www.ffiec.gov
Finlande	Bureau de protection des données Ombudsman	www.tietosuoja.fi
France	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr
Grèce	Autorités Helleniques de Protection des données	www.dpa.gr
Hongrie	Adatvédelmi Biztos	www.obh.hu
Islande	Persónuvernd	http://www.personuvernd.is
Italie	Garante per la protezione dei dati personali	www.garanteprivacy.it
Japon	Cabinet du Premier Ministre	http://www5.cao.go.jp/seikatsu/kojin/index/html
	Ministères compétents (pour le secteur privé)	
Luxembourg	Commission nationale pour la protection des données	www.cnpd.lu
Norvège	Datatlsynet	www.datatilsynet.no/
Nouvelle Zélande	Privacy Commissioner	www.privacy.org.nz
Pays Bas	College Bescherming Persoonsgegevens	www.cbpweb.nl
	OPTA – Autorité indépendante des postes et télécommunications	www.opta.nl

Tableau 1. Autorités d'application pour la protection de la vie privée au niveau national dans les pays de l'OCDE
(Suite)

Pologne	Inspecteur Général pour la protection des données à caractère personnel	www.giodo.gov.pl
Portugat	Commission nationale de protection des données	www.cnpd.pt
République slovaque	Bureau de protection des données à caractère personnel	www.dataprotection.gov.sk
République tchèque	Bureau pour la protection des données à caractère personnel	www.uoou.cz
Royaume-Uni	Information Commissioner	www.ico.gov.uk
Suède	Datainspektionen	www.datainspektionen.se
Suisse	Préposé fédéral à la protection des données	www.edsb.ch

On peut noter certaines spécificités dans les systèmes des États-Unis, du Japon et de la Corée. Aux États-Unis, la protection de la vie privée dans le secteur privé est traitée en partie comme un aspect de la protection des consommateurs assurés par le *Federal Trade Commission* par des dispositions de longue date interdisant les pratiques déloyales et trompeuses dans les relations commerciales. Un rôle parallèle est joué par le *Department of Justice for criminal proceedings*. Mais dans le cadre de la tradition législative de la *Common law*, les États-Unis se sont également dotés de législations sectorielles et thématiques spécifiques, par exemple dans les secteurs de la santé ou des services financiers, qui confient aussi bien à d'autres organismes fédéraux l'application de la protection de la vie privée. L'application de la protection de la vie privée est également assurée au niveau des États fédérés.

Le Japon et la Corée ont donné des réponses concernant à la fois le secteur public et le secteur privé. Dans le secteur public, la protection des données est mise en oeuvre par les ministères. En Corée, le ministère de l'administration gouvernementale et de l'intérieur a un pouvoir général de surveillance de la protection des données dans les organismes administratifs. Au Japon, la législation prévoit que les différents types d'organismes administratifs doivent respecter la vie privée et la réglementation en matière de protection de la vie privée. Son application est assurée par le système judiciaire. Ces deux pays disposent de législations visant le secteur privé. Au Japon, le Cabinet du Premier ministre a la responsabilité générale de veiller à la protection de la vie privée, mais les plaintes sont traitées par le Centre national de la consommation et par d'autres organismes. Les ministres concernés peuvent promulguer des décrets d'application visant les secteurs industriels sur lesquels ils ont compétence. En Corée, les principales autorités d'application sont le Ministère de l'information et des communications qui est doté de larges pouvoirs afin de protéger la vie privée dans le cadre des communications électroniques et le KISA, dont les pouvoirs ne découlent pas d'une législation cadre mais sont néanmoins très larges dans la mesure où ils s'appliquent également aux données à caractère personnel dans les communications électroniques.

Plaintes et traitement des plaintes

La résolution des problèmes des particuliers a toujours été considérée comme un élément important de l'action des autorités chargées de la vie privée et de la protection des données. Dans certains domaines de la réglementation, la résolution des plaintes est habituellement prise en charge par le Médiateur ou par d'autres services, tandis que les autorités d'application traitent plutôt les personnes qui déposent des plaintes comme des informateurs fournissant des éléments de preuve pouvant être utilisés à l'appui d'une action de sanction. Dans le contexte européen, la Directive européenne suggère, sans l'imposer, que ces deux fonctions soient exercées de concert. La Corée a adoptée une autre approche en établissant un Comité de médiation des différends en matière d'information à caractère personnel au sein du KISA afin de contribuer à la résolution des différends touchant la vie privée.

Il était demandé dans l'enquête d'indiquer si les autorités étaient habilitées à recevoir des réclamations des particuliers relatives à des violations les concernant en vue d'y apporter une solution. Chacun des pays répondants dispose d'au moins une autorité habilitée à examiner les plaintes relatives à la vie privée. L'Allemagne a fourni des informations sur plus d'une vingtaine d'autorités fédérales et locales indépendantes. La plupart des pays ne limitent pas à leurs ressortissants ou aux résidents le droit de présenter des plaintes. Néanmoins, en Albanie et en Suisse il existe une réglementation prévoyant que pour présenter une plainte il faut être ressortissant ou résident légal du pays. En Nouvelle-Zélande, l'Autorité ne peut pas donner suite à la requête d'accès d'un ressortissant étranger présentée depuis l'étranger.

Toutes les autorités peuvent recevoir des plaintes par courrier classique, et presque toutes par téléphone ou en ligne. En Italie la loi dispose expressément que certains types de plaintes doivent être présentées par écrit, bien que des plaintes informelles, dans lesquelles un individu agit comme informateur, puissent être faites par téléphone ou par courrier électronique. L'Australie, la Belgique, l'Espagne, la Pologne et le Royaume-Uni font partie des exceptions qui n'acceptent pas les plaintes par téléphone. Cette attitude envers les plaintes par téléphone se retrouve dans nombre d'autres réponses. Même lorsque de telles plaintes sont possibles, elles ne sont souvent pas encouragées comme dans le cas de l'Autriche ou doivent faire l'objet d'une confirmation écrite comme dans le cas de la France. Les variations dans les réponses doivent être probablement mises sur le compte du niveau de développement des systèmes individuels dans les différents pays, du poids accordé à la démonstration du caractère authentique d'une plainte et sur les différentes définitions retenues du terme plainte.

Une faible majorité d'autorités signalent avoir l'obligation de faire enquête en cas de plainte. Les contours précis de ce que recouvre cette obligation peuvent cependant varier. Le Commissariat fédéral canadien a l'obligation de faire enquête mais peut refuser d'émettre un rapport pour diverses raisons telle que l'existence de mesures correctives alternatives ou à cause du caractère frivole ou vexatoire de la plainte. De même, en Australie et en Nouvelle-Zélande les commissaires sont dotés d'un pouvoir discrétionnaire limité pour interrompre ou ne pas entamer une enquête. La Belgique fait une distinction entre le fait que son autorité a l'obligation de traiter une plainte mais qu'elle n'est pas nécessairement tenue de mener une enquête.

Dix-huit réponses ont fourni des statistiques sur les plaintes ou ont renvoyé à des informations contenues dans des rapports publiés par les autorités nationales. En raison de différences dans les pratiques de classification, il s'avère difficile de procéder à des analyses comparatives internationales. Toutefois, certaines observations peuvent être réalisées. Le Canada et l'Italie semblent représentatifs, dans la mesure où le secteur financier figure de façon prédominante dans les plaintes touchant les organisations du secteur privé. Par contre, en France, plus d'un quart des plaintes concerne les télécommunications ou l'audiovisuel. Les télécommunications et le secteur financier prédominent également en Australie, en Espagne, en Islande et en Pologne. La Nouvelle-Zélande et la Hongrie ont indiqué que les plaintes contre le gouvernement étaient plus fréquentes que les plaintes contre les organisations du secteur privé. La FTC américaine collecte et analyse les plaintes concernant les usurpations d'identité. En 2005, les fraudes relatives aux cartes de crédit (26%) étaient la forme la plus courante d'usurpation d'identité suivies des fraudes en matière de services téléphoniques ou autres services publics (18%), des fraudes bancaires (17%) et des fraudes en matière d'emploi (12%).

Enquêtes, vérifications et inspections

L'enquête demandait aussi des informations sur les pouvoirs et activités considérés davantage sous l'angle du contrôle réglementaire que de la résolution des plaintes. Il s'agit notamment des études ou des vérifications destinées de façon générale à s'assurer du respect de la réglementation par une organisation ou un secteur industriel, ainsi que des investigations sur de possibles violations de la vie privée en vue d'imposer les sanctions appropriées. Dans ce domaine, les pouvoirs des autorités sont très variés. Par exemple, au Royaume-Uni, le Commissaire ne peut procéder à des vérifications qu'avec le consentement du maître du fichier, à quelques exceptions près, alors que beaucoup d'autres autorités sont habilitées à mener des vérifications contraignantes. En revanche, il est l'un des rares qui soit habilité dans certaines enquêtes criminelles à pénétrer dans des locaux privés sans préavis, avec un mandat de perquisition. En général il s'agit d'un domaine où la culture juridique d'un pays est susceptible d'influer sur la manière dont ces pouvoirs seront accordés aux autorités d'application.

Le questionnaire portait également sur les compétences des autorités à lancer des investigations de leur propre initiative et à mener des vérifications et des inspections. Seul le KISA a indiqué qu'il n'était pas habilité à faire enquête de sa propre initiative alors que le Ministère coréen de l'information et de la communication (MIC) peut le faire. Ainsi en règle générale les autorités combinent les rôles de traitement des plaintes et de régulateur ou d'« exécuteur ». L'enquête ne nous permet pas de tirer des conclusions sur la façon dont les autorités gèrent la tâche difficile d'arbitrer entre ces rôles et la priorité qu'elles accordent toutes soit à répondre aux individus soit à veiller au respect de la réglementation. Ce double rôle a posé des problèmes à certaines autorités.[43]

Beaucoup d'autorités semblent avoir des pouvoirs très larges pour la conduite de leurs investigations. La plupart des autorités peuvent exiger d'un responsable d'un traitement de données qu'il communique des informations et des documents. Un groupe plus réduit d'autorités, qui exclut le Japon, la Corée, le Royaume Uni et bien sûr les états allemands, a des pouvoirs similaires en ce qui concerne les relations avec des tiers. De même, la plupart, si ce n'est la totalité, des autorités peuvent pénétrer dans des locaux privés sans le consentement des intéressés. L'exercice de ce pouvoir nécessite souvent un mandat de perquisition comme dans le cas de l'Australie, de la France, de l'Italie, du Royaume Uni et des États-Unis. Il a également été indiqué qu'une grande majorité des autorités pouvait demander la cessation temporaire ou définitive du traitement de données mais dans ce cas l'ampleur des formalités légales nécessaires n'est pas toujours très claire.

Le point relatif à la conduite des investigations concerne la capacité des autorités à mener des vérifications ou des inspections sur site. C'est un pouvoir habituel des autorités d'application mais il n'est pas universel – la FTC américaine, le KISA et les ministères japonais compétents n'en disposent pas. Lorsqu'ils existent, ces pouvoirs se répartissent en deux groupes : dans le premier groupe, l'utilisation de ces pouvoirs est entourée de protections et de limites. Par exemple le Royaume-Uni exige habituellement le consentement du responsable du traitement des données alors que les autorités en Albanie, Belgique, Canada, Hongrie, Italie, et le MIC coréen demandent des motifs raisonnables de croire que la législation n'a pas été respectée. Mais ces protections ne sont pas universelles. Dans le second groupe d'autorités de la République Tchèque, la France, l'Allemagne, l'Islande, les Pays-Bas et la Pologne, les pouvoirs semblent avoir peu de limites formelles. Plusieurs répondants ont noté que bien qu'il n'avait pas d'exigence formelle, il était de pratique courante d'informer le responsable du traitement de données à l'avance d'un audit à moins qu'il n'existe une raison grave de ne pas le faire.

Sanctions, dédommagements et résultats[44]

L'enquête s'est également intéressée aux sanctions qui peuvent être imposées par les autorités d'application ou demandées par elles par voie judiciaire. En ce qui concerne les dédommagements proposés aux personnes concernées, seuls quatre répondants ont indiqué le pouvoir d'aider la personne a intenter des procédures judiciaires et trois répondants seulement ont indiqué le pouvoir d'entreprendre un arbitrage obligatoire. Dans onze cas, cependant, les réponses à l'enquête ont indiqué qu'une médiation pouvait être entreprise, et l'autorité d'un état allemand a fait remarquer qu'à son avis des mesures volontaires telles que la médiation pouvaient toujours être entreprises.

Dix-neuf répondants ont indiqué disposer du pouvoir de décider s'il y a violation de la législation, mais dans dix cas seulement une telle décision a un effet juridique par elle-même. En revanche 15 autorités peuvent émettre des mises en garde ou des réprimandes et toutes sauf deux sont autorisées à rendre publiques les violations. Toutes les autorités allemandes sont habilitées à rendre publiques les violations ou et à émettre des mises en garde ou des réprimandes.

Seules six autorités disposent du pouvoir de négocier des amendes ou autres formes de règlements. La FTC américaine dispose de tels pouvoirs avec la procédure des jugements d'expédient. Le Commissariat fédéral canadien peut tenter de résoudre des plaintes par la médiation et la conciliation, qui peuvent déboucher sur un accord. Le Commissaire australien considère que les accords négociés sont le meilleur moyen de résoudre les plaintes. La République tchèque, les Pays-Bas et le MIC coréen font également partie de ce groupe restreint. La France a cependant indiqué qu'une autorité de régulation qui peut imposer une décision n'a pas besoin de négocier d'accords – réponse qui peut sans doute s'appliquer aux autres autorités qui disposent de forts pouvoirs d'exécution.

Une majorité – c'est-à-dire 16 autorités sur les 24 étudiées –peut prononcer des décisions légalement exécutables. Au Japon et en Corée ces actions sont prises par le ministre plutôt que par une autorité d'application chargée des plaintes. Les autorités allemandes peuvent émettre des ordres ayant force exécutoire uniquement par rapport au secteur privé.

Seules trois pays –Australie, Norvège et les États-Unis – ont des autorités qui peuvent ordonner que des indemnités soient versées aux particuliers. Dix autorités peuvent solliciter des injonctions auprès d'un tribunal et 16 d'entre elles peuvent solliciter des pénalités de nature financière ou autres. Sept autorités ont le pouvoir d'intenter des procédures pénales. Toutefois, il semblerait que les autres peuvent soumettre une demande officielle auprès des autorités chargées des poursuites pénales. Le Commissaire du Royaume-Uni est le seul qui conduit ses propres poursuites devant les juridictions pénales d'Angleterre, du pays de Galles et d'Irlande du Nord. Alors qu'en Écosse, les affaires sont renvoyées auprès de l'autorité chargée des poursuites pénales selon un schéma plus conforme à celui qu'on retrouve au sein de l'OCDE.

La seconde partie de l'enquête sur les sanctions concernait les dédommagements prévus dans le cadre du processus judiciaire. Il était demandé d'indiquer les pouvoirs d'injonction, d'indemnisation de la personne concernée, de pénalités civiles, d'amendes pénales et de condamnation à des peines d'emprisonnement à la suite d'une condamnation pénale. L'ensemble des répondants offre certaines voies de recours par le biais des tribunaux de droit commun ou de tribunaux spéciaux. Parfois, les recours judiciaires compensent l'éventail limité des sanctions pouvant être imposées par l'autorité. Ainsi, par exemple, le KISA disposent de pouvoirs plutôt limités mais un grand nombre de sanctions peuvent être prononcées par les tribunaux coréens y compris l'indemnisation des personnes concernées et des amendes et des peines d'emprisonnement en cas de condamnation pénale. Seize des 24 réponses indiquaient que les tribunaux pouvaient imposer des amendes administratives. En Allemagne, au niveau des états, dans la plupart des cas toute la gamme des sanctions peut être prononcée par les tribunaux, mais, au niveau fédéral, seules des injonctions peuvent être requises.

Les sanctions disponibles en cas de non respect de la législation varient considérablement. En République Tchèque et en Islande, les autorités peuvent imposer des astreintes quotidiennes et au Danemark, le contrevenant est déféré à la police. Lorsqu'il y a violation d'une décision d'un tribunal, la réponse classique est l'application des mécanismes habituels d'exécution des décisions judiciaires. La Belgique et la France ont répondu que les méthodes normales d'exécution des décisions judiciaires s'appliqueraient, ce qui serait également le cas pour les décisions judiciaires en Nouvelle-Zélande et en Pologne. L'Espagne a déclaré faire appel au système fiscal pour recouvrer les amendes impayées et l'Albanie a également mentionné la possibilité de faire rapport au Parlement à titre de sanction supplémentaire. L'Australie, le Canada et les États-Unis ont expressément mentionné la possibilité de faire usage des procédures d'atteinte à l'autorité du tribunal.

B. Législations nationales sur la vie privée

Bien que ce projet mette l'accent sur la capacité des autorités chargées de l'application des lois sur la vie privée à fonctionner dans un environnement transfrontière, le questionnaire demandait également des informations de base sur les lois relatives à la vie privée que ces autorités étaient chargées de faire appliquer. Il était demandé si les lois étaient d'application générale ou de nature sectorielle et si elles abordaient les principes suivants sur la vie privée :

- Ouverture/transparence.
- Qualité des données.
- Collecte et utilisation.
- Garanties de sécurité.
- Accès de la personne concernée.
- Flux transfrontières de données.

Les pays de l'EEE possèdent des lois d'application générale, à quelques exceptions près. C'est-à-dire que même si la Directive européenne ne s'applique pas aux secteurs de la justice et de l'intérieur ni aux autres secteurs qui ne font pas partie du champ de compétence de la communauté, les membres de l'EEE couvrent souvent au moyen d'une législation unique les secteurs qui sont visés par la Directive et ceux qui ne le sont pas. Quoiqu'il en soit, les membres de l'Union européenne ont l'obligation de disposer d'une législation sur la protection des données pour les secteurs de la justice et de l'intérieur qui soit conforme aux dispositions de la Convention 108.[45] Les Pays-Bas ont communiqué des informations sur les lois appliquées à la fois par l'autorité générale de protection des données et par l'autorité de régulation des télécommunications. Pour le secteur privé, l'Allemagne a une loi uniforme et substantive au niveau fédéral. Le gouvernement fédéral et les États ont leurs propres dispositions en place pour le traitement de données dans l'administration publique. De même, grâce à son corpus de législations fédérales et provinciales, le Canada dispose d'un ensemble de lois s'appliquant généralement aux secteurs public et privé. En revanche, bien que l'Australie dispose d'un ensemble de lois assez complet au niveau fédéral, celui-ci définit des principes différents pour les secteurs public et privé et pour les questions spécifiques des dossiers de crédit, des déclarations fiscales et des condamnations exécutées. Le Japon et la Corée traitent différemment les secteurs public et privé et l'analyse a surtout porté sur la législation visant le secteur privé. La FTC américaine est principalement une agence de protection des consommateurs et la protection de la vie privée ne constitue qu'une partie de sa mission plus large de protection des consommateurs.

Dans leur ensemble, les législations des pays de l'EEE mettent en œuvre les six catégories de principes susmentionnées. La série de lois sectorielles dont la FTC veille à l'application est trop complexe pour être traitée dans le cadre de ce rapport. Le Japon et la Nouvelle-Zélande cherchent à couvrir l'ensemble des domaines à l'exception des flux transfrontières de données; la Corée aborde l'ensemble des

cinq catégories. Au Canada, la loi fédérale sur la protection des renseignements à caractère personnel qui s'applique au secteur public n'aborde pas les questions de sécurité ou les flux transfrontières de données.

Même lorsque les lois nationales essaient d'appliquer des principes identiques, des différences d'interprétation reflétant les différences historiques, culturelles et juridiques peuvent entraver la coopération entre les autorités. Toutefois, en mettant l'accent sur les faits qui sont à l'origine des plaintes on peut contribuer à réduire les tensions entre les différentes catégories juridiques.

SECTION II. ASPECTS TRANSFRONTIÈRES DE L'APPLICATION DE LA LÉGISLATION POUR LA PROTECTION DE LA VIE PRIVÉE

La seconde partie du questionnaire portait sur les aspects « transfrontières » de l'exécution. Ce terme est utilisé dans un sens large et s'applique aux cas où « la personne concernée par les données est établie dans un pays différent de celle qui contrôle ces données, où les données elles-mêmes ont été transmises à un pays tiers, ou simplement aux cas où des données importantes se trouvent dans un pays tiers. » Les travaux de l'OCDE sur l'application de la législation dans d'autres domaines (protection des consommateurs, spam) ont mis en évidence des défis considérables qu'il fallait maîtriser pour pouvoir opérer efficacement dans un contexte transfrontière. Les résultats du questionnaire suggèrent que la situation est similaire dans le cas de la vie privée, bien que l'on dispose peut-être d'une moins grande expérience pratique d'exécution pour former une appréciation.

L'expansion continue de l'utilisation de l'Internet et la nature évolutive des flux transfrontières de données suggèrent que le besoin pour les autorités d'application de s'attaquer aux problèmes transfrontières ne va aller qu'en augmentant. Dès à présent, la Commission européenne a identifié les flux transfrontières de données comme un domaine dans lequel le manque d'intervention en matière d'application semble créer un fossé entre la législation et la pratique.[46] C'est un sentiment semblable qu'exprime un praticien qui a observé que la nature mondiale de l'Internet signifie que « dans bien des cas il existe un fossé entre les exigences applicables en matière de protection des données et la possibilité pour les autorités de faire appliquer ces exigences ».[47] Cette section du présent rapport décrit plusieurs activités d'application transfrontières, ainsi que les défis juridiques et pratiques qu'un environnement transfrontière soulève pour les autorités d'application.

A. Exemples d'activité d'application transfrontière

Litiges transfrontières

Bien qu'ils ne soient pas très courants, il y a cependant eu plusieurs exemples d'intervention transfrontière. Il y a eu ainsi au Royaume-Uni deux affaires distinctes dans lesquelles des violations alléguées de l'interdiction d'obtenir des données à caractère personnel par des moyens fallacieux ont nécessité une assistance transfrontière. Dans le premier cas il a fallu faire appel à un expert sur la législation d'un pays du Moyen-Orient et également mener des investigations en France. Dans le second il a fallu mener des investigations en Norvège, et dans ce cadre l'assistance de l'autorité norvégienne de protection des données a été sollicitée en vertu de la Convention 108 et de l'accord de l'EEE qui rend applicable la Directive de l'Union européenne à la Norvège. La Corée a indiqué qu'en février 2006, les noms et numéros d'enregistrement de résident de 250 000 Coréens ont été volés dans un jeu en ligne très populaire par des pirates informatiques basés en Chine. A ce jour, les victimes n'ont pas subi de dommages financiers, mais un risque existe car les numéros d'enregistrement peuvent être utilisés pour acquérir d'autres données privées et les autorités coréennes ont éprouvé des difficultés à établir une coopération avec les autorités chinoises concernées. Naturellement, les règles applicables aux flux transfrontières de données ont également générées certains litiges. Par exemple, l'Islande indique qu'en 2005 l'autorité de protection des données a conclu que l'envoi de prélèvements sanguins aux États-Unis équivalait au transfert de données à caractère personnel à l'étranger et en conséquence exigé l'application des règles relatives aux flux transfrontières de données.

On peut trouver d'autres exemples de procédures transfrontières dans les relations entre le Canada et les États-Unis. Le Bureau de la Commissaire à la protection de la vie privée du Canada a lancé une enquête à la suite de l'obtention par une revue canadienne des relevés téléphoniques de la Commissaire à la protection de la vie privée et d'un autre membre du personnel auprès d'un courtier de données basé aux États-Unis. Ce courtier de données avait obtenu les relevés auprès d'au moins 2 sociétés canadiennes différentes de télécommunications. Parmi d'autres exemples, on trouve une affaire impliquant un site Internet basé aux États-Unis (Abika.com) fournissant sans leur consentement des profils psychologiques et des recherches sur les casiers judiciaires de citoyens canadiens. La Commissaire à la protection de la vie privée du Canada a conclu qu'elle ne pouvait pas donner suite à la plainte au motif qu'elle n'avait pas suffisamment compétence pour enquêter. La FTC américaine a entamé une procédure de mise en demeure contre les opérateurs du même site Internet en alléguant une violation de la vie privée contraire à la loi américaine.[48] Parmi d'autres exemples canado américains on retrouve des plaintes relatives au transfert vers les États-Unis d'informations de cartes de crédit pour traitements par un tiers.

Bien que le petit échantillon d'affaires présenté ci-dessus ne soit pas forcément représentatif, il donne une image des situations auxquelles sont confrontées les autorités. Une enquête plus vaste pourrait permettre de découvrir d'autres cas transfrontières peut-être en nombre réduit – mais d'importance et posant des problèmes. La poursuite des recherches dans ce domaine est difficile parce que dans de nombreux pays les affaires d'atteinte à la vie privée passent rarement devant les tribunaux et il n'y a souvent pas de rapports accessibles sur l'issue des litiges relatifs à la vie privée à moins qu'ils ne soient établis par les autorités d'application. L'identification des litiges ayant une dimension transfrontière est encore plus difficile dans la mesure où ce facteur n'est souvent pas mentionné dans les comptes rendus ou les articles de presse.

Vérifications ou inspections ayant une dimension transfrontière

La coopération tend à se développer au plan international en ce qui concerne les investigations réglementaires. Le groupe de conseil européen pour la protection des données, aussi connu sous le nom de Groupe de travail sur la protection des données (Article 29)[49] a défini des critères pour le choix des activités ou secteurs à examiner et a décidé qu'il allait entreprendre en 2005 et en 2006 des investigations nationales coordonnées. Suite à cette déclaration, le secteur de l'assurance santé privée a été retenu comme l'objet de cette première série d'actions et un questionnaire a été préparé en vue d'obtenir des informations de la part des sociétés oeuvrant dans ce secteur. Le Groupe de travail « Article 29 » a aussi mené des vérifications conjointes des modalités relatives à l'échange des données PNR (Passager Name Records) sur les passagers entre les compagnies aériennes européennes et les autorités douanières et frontalières de l'Australie, du Canada,[50] et des États-Unis.[51]

Un autre exemple transfrontalier concerne l'examen des conséquences sur la vie privée des services Web Passeport de Microsoft au sujet desquels plusieurs autorités européennes ont reçu des plaintes identiques. Une analyse conjointe a été organisée par l'intermédiaire du Groupe de travail « Article 29 ».[52] Il s'agit d'un exemple tout à fait symptomatique, car la FTC américaine a également reçu des plaintes, a examiné des problèmes connexes et fait fléchir Microsoft.[53] Dans la limite de leurs pouvoirs, la FTC et les autorités européennes ont tenté de s'informer mutuellement de leur progrès, de leur décision et de leurs raisonnements respectifs.

B. Problèmes juridiques et pratiques pour une application transfrontière efficace

Responsables de traitement des données étrangers ou personnes concernées étrangères

Le questionnaire demandait si les autorités peuvent prendre des mesures contre un responsable du traitement des données situé à l'étranger ou pour protéger les données concernant des personnes étrangères. Quatorze répondants ont dit que leurs autorités pouvaient prendre des mesures contre les responsables d'un traitement de données à l'étranger. Le Danemark, l'Espagne, la France, l'Italie, la Norvège, la Pologne et le Royaume-Uni ont fait clairement référence aux dispositions de leur législation nationale transposant la Directive de l'Union européenne qui leur enjoignent d'exercer leurs compétences à l'encontre des responsables d'un traitement de données établis sur leur territoire ou qui utilisent des équipements situés sur leur territoire pour le traitement de données à caractère personnel à des fins autres que de transit. Cette obligation vaut pour l'ensemble des pays membres de l'Union européenne ainsi que les autres membres de l'EEE. L'Australie, le Japon et la Suisse ont indiqué qu'ils ne pouvaient pas agir contre les responsables d'un traitement des données situés à l'étranger ; la Nouvelle-Zélande a déclaré que les pouvoirs de son autorité en pareilles circonstances ne sont pas clairs ; le Canada et la FTC américaine peuvent agir sous réserve que le responsable du traitement des données ait un lien de rattachement suffisant avec leur pays. De plus amples informations pourraient être nécessaires pour déterminer si les limites se rapportent à la compétence juridique, ou sur la capacité à agir en pratique contre le responsable d'un traitement de données situé à l'étranger ? Par ailleurs, tous les États à l'exception des autorités coréennes peuvent agir contre un résident responsable d'un traitement de données en vue de protéger les données concernant une personne étrangère.

Notification et échange d'information

Le questionnaire demandait si les autorités pouvaient notifier aux autorités d'autres pays les enquêtes qui pourraient les affecter et si elles pouvaient échanger des informations avec ces autorités étrangères. Dix-huit répondants ont indiqué que les autorités de leur pays pouvaient à la fois notifier les autorités étrangères et partager des informations avec elles. Quatorze des 18 autorités appartiennent à des pays membres de l'EEE et beaucoup d'entre elles ont indiqué que la Convention 108 et la Directive de l'Union européenne les obligeaient à coopérer avec les autres autorités et en particulier à échanger des informations avec elles.

A l'extérieur de l'Europe, le Canada a indiqué qu'il n'était pas habilité, sauf dans des circonstances spécifiques, à notifier des autorités étrangères ou à échanger des informations. La FTC américaine peut notifier d'autres autorités et échanger des informations, mais fortement préoccupée des restrictions par les limitations de ses compétences sur ce point, elle a demandé un élargissement de ses pouvoirs par la voie législative. La Nouvelle-Zélande n'est pas certaine de pouvoir échanger des informations. Au Japon, la législation couvrant le secteur privé ne prévoit pas ni la notification, ni l'échange d'information ni l'assistance en matière d'enquête. En Corée, le KISA ne peut pas notifier les autorités étrangères mais il peut dans certaines circonstances fournir des informations sur les affaires dans lesquelles la vie privée d'une personne résidente a été violée par un responsable de traitements de données situé à l'étranger.

Il semblerait donc que même si de nombreuses autorités sont habilitées à échanger des informations, ces pouvoirs sont spécifiquement encadrés et limités et semble fonctionner au mieux entre les membres de mêmes groupes de pays tels que les États parties à la Convention 108. Le pouvoir d'échanger des informations à l'extérieur de tout groupement officiel n'est pas garanti et cette incertitude préoccupe les autorités d'application. Pour lever les restrictions à l'échange d'information il faudrait dans certains cas revoir la législation ou la réglementation pertinente mais cela est un élément crucial pour permettre une coopération internationale efficace.

Autres problèmes

Seize réponses sur 24 indiquaient clairement que l'absence de pouvoir était un obstacle et 15 réponses ont indiqué que les restrictions à l'échange d'information étaient un obstacle particulier. Seize autorités ont mentionné l'incompatibilité des régimes juridiques ; onze autorités ont noté le problème des ressources inadéquates ; mais seules trois d'entre elles ont indiqué que la langue constituait un obstacle.

Dans le domaine de l'application de la législation sur la protection de la vie privée comme dans d'autres domaines de coopération juridique transfrontières, il faut noter que lorsque des ordonnances ont été prononcées ou des sanctions imposées, se pose la question de la reconnaissance et de l'exécution des décisions transfrontières.[54] Cela pose un problème pour l'exécution des décisions judiciaires que ce soit en faveur d'individus ou d'une autorité, et le problème est peut-être encore plus aigu pour les sanctions imposées dans le cadre d'un processus administratif.

La difficulté d'identifier un point de contact ainsi que la diversité des priorités en matière d'exécution ont également été mentionnées. Par rapport à la question du point de contact, chacun des pays ou presque a déclaré qu'il avait ou pouvait mettre en place un point de contact unique.[55] D'après les réponses une moitié seulement des autorités ont défini des priorités en matière d'exécution. Dans un cas, ces priorités ont été décrites par rapport aux secteurs choisis comme cible pour mener une action réglementaire. Lorsqu'une autorité a défini des priorités d'exécution celles-ci semblent habituellement décrites en termes généraux. D'après l'information limitée disponible, les comportements récidivistes, la gravité des dommages et le nombre d'individus affectés semblent être les critères de plus communément retenus. La France fait exception dans la mesure où elle donne priorité à des affaires répondant à des préoccupations politiques actuelles telles que la biométrie et la vidéosurveillance.

C. Mécanismes existants pour la coopération transfrontière dans l'application de la législation sur la vie privée

Les activités et les rapports des autorités de protection des données et de la vie privée font clairement apparaître que celles-ci attachent une importance considérable aux mécanismes de coopération internationale et régionale. Les résultats de l'enquête font également clairement apparaître que les autorités se préoccupent effectivement de leur capacité juridique à prendre part à ces activités conjointes. Lorsque il existe un cadre juridique permettant ou enjoignant de faire appel à la coopération, comme dans le cas de l'Europe, ces mécanismes sont utilisés d'une part dans un nombre restreint d'affaires individuelles et d'autre part pour faciliter des actions de régulation conjointes plus larges. En raison du chevauchement des appartenances à l'OCDE, à l'UE, au Conseil de l'Europe et à l'APEC, il sera certainement bénéfique de poursuivre l'échange d'information et la coordination des travaux en cours.

Instruments internationaux pour la coopération sur la protection de la vie privée

Conseil de l'Europe

L'importance de la coopération en matière d'exécution a été reconnue par les autres institutions internationales qui ont élaboré des instruments relatifs à la protection des données. Le Conseil de l'Europe a œuvré parallèlement à l'OCDE à la fin des années 1970 et en janvier 1981 a ouvert à la signature sa Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.[56] Le modèle choisi par le Conseil de l'Europe était l'adoption d'un ensemble de principes de base. Il comporte également des règles spéciales en matière de flux transfrontières de données (FTD) et des mécanismes d'assistance mutuelle. Les principes fondamentaux ont été repris des résolutions antérieures du Comité des ministres et de la législation des États membres. Parmi ces principes on retrouvait les règles désormais familières sur la qualité des données (par exemple licéité et loyauté dans

l'obtention et le traitement), les données sensibles, la sécurité et les droits de individus, et ils reproduisaient étroitement les principes des Lignes directrices de l'OCDE. Des droits de dérogation limités ont été repris de l'Article 8 de la Convention européenne des droits de l'homme,[57] et des dispositions ont été introduites limitant le droit des parties d'interdire ou de restreindre les flux transfrontières de données pour des raisons tenant à la protection des données. La Convention prévoit que des États non membres du Conseil de l'Europe puissent y accéder. La Convention s'est révélée le principal moteur au plan international pour la protection des données en Europe au cours des années 1980 et au début des années 1990. Un protocole ultérieur est venu modifier la Convention pour aligner ses dispositions relatives aux FTD et aux autorités de supervision avec celles de la Directive de l'Union européenne.

Le chapitre IV de la Convention 108 comprend des dispositions détaillées relatives à l'assistance mutuelle, qui par commodité sont reproduites dans l'Annexe D. L'article 13 prévoit l'obligation générale de fournir une assistance mutuelle y compris l'obligation de nommer au moins une autorité chargée de ces questions, qui n'a pas obligatoirement à être une autorité chargée spécialement de la protection des données, l'obligation principale étant de fournir l'information. L'article 14 impose l'obligation de fournir assistance aux résidents étrangers. L'article 15 impose des restrictions sur l'utilisation pouvant être faite des informations obtenues dans le cadre de l'entraide et l'Article 16 fournit une liste complète de motifs pour lesquels l'assistance peut être refusée. L'article 17 établit les coûts et les procédures en matière d'assistance. En outre, le chapitre V de la Convention met en place un Comité consultatif (le T-PD) qui sert de forum d'échange sur les enjeux et les évolutions de la protection de la vie privée. Bien que les documents publics n'y fassent pas beaucoup écho, l'expérience des régulateurs montre que ces dispositions ont été utilisées, peut-être pas fréquemment ou complètement, mais régulièrement au cours des années.

Ce chapitre de la Convention a servi de base à la coopération entre de nombreux États européens avant l'adoption de la Directive 95/46/CE de l'Union européenne. Il organise toujours la coopération dans les domaines qui ne sont pas couvert par la Directive, comme les questions de police et dans les cas où un État ne ferait pas partie de l'EEE mais aurait ratifié la Convention.

Union européenne

C'est sans doute dans la Directive de l'Union européenne adoptée en octobre 1995 qu'on retrouve les obligations de coopérer les plus rigoureuses (Directive 95/46/CE).[58] La Directive exige la mise en place d'autorités nationales de supervision, leur impose des obligations en matière de coopération et créé un mécanisme de coopération. Ces dispositions ont peu à peu dominé les mécanismes de coopération au sein de l'Europe. L'article 28 de la Directive de l'UE exige expressément la mise en place d'autorités nationales de supervision. Ces autorités doivent être dotées de pouvoir d'enquête, de pouvoir effectifs d'intervention et du pouvoir d'entamer des procédures judiciaires. Les autorités sont habilitées à examiner les plaintes et à mener des vérifications en matière de traitement de données à caractère personnel. Dans le contexte actuel, les dispositions permettant de demander aux autorités de déléguer leurs pouvoirs à d'autres autorités des États membres de l'EEE et l'obligation prévue de coopération entre autorités présentent un intérêt particulier. L'article 29 de la Directive de l'Union européenne établit un Groupe de travail composé en grande partie des autorités de supervision des États membres prévu à l'article 28. Le rôle du Groupe de travail est pour une large part de conseiller la Commission Européenne mais il est devenu au fil du temps un des outils principaux permettant d'établir une position commune au sein des autorités européennes de protection des données et plus récemment pour les opérations conjointes d'exécution.

Bien que ces instruments du Conseil de l'Europe et de l'UE constituent une importante base pour la coopération au sein de l'Europe et soient mentionnés par les répondants au questionnaire, on ignore dans quelle mesure l'information peut être échangée à l'extérieur de ces groupements. Il est possible que l'échange d'information ne soit absolument pas autorisé ou le soit simplement dans le cadre de sa propre enquête. Cela est particulièrement probable au sein de l'EEE parce que, dans ces pays, les autorités de

supervision de la protection des données sont soumises à une obligation de secret professionnel imposée par l'article 28.7 de la Directive de l'UE. Les dispositions de la Directive 95/46/CE relatives à la coopération en matière d'exécution sont reproduites en Annexe C.

En 2002 la Commission Européenne a convoqué une conférence pour examiner son premier rapport sur la transposition de la Directive européenne.[59] A la suite de cet examen, la Commission a adopté un plan d'action qui encourageait une application plus systématique de la Directive au sein de l'UE. En novembre 2004 le groupe de travail Article 29 a déclaré que 'la mise en application est un instrument important dans la "boite à outils" de la conformité', et a également fait part de son intention d'adopter une attitude plus proactive envers la mise en application de la législation relative à la protection des données dans l'Union européenne.[60]

Coopération Économique Asie Pacifique

En novembre 2004, Les ministres de la Coopération économique de l'Asie Pacifique, ont adopté le cadre de confidentialité de l'APEC, élaboré par son groupe de pilotage sur le commerce électronique :

> « Conformément au lignes directrice de l'OCDE sur la protection de la vie privée de 1980, les principes et Lignes directrices relatives à la mise en oeuvre du cadre de confidentialité sont axés sur les quatre objectifs principaux suivants :
>
> – Élaborer des mesures appropriées de protection de la confidentialité des informations à caractère personnel.
>
> – Empêcher la création d'obstacles inutiles à la circulation de l'information.
>
> – Permettre aux entreprises multinationales de mettre en œuvre des approches uniformes en matière de collecte, d'utilisation et de traitement des données ; et
>
> – Faciliter les efforts nationaux et internationaux en vue de promouvoir et mettre en oeuvre des mesures de protection de la confidentialité de l'information. »[61]

L'un de ces quatre objectifs couvre la facilitation des efforts internationaux en vue de mettre en oeuvre des mesures de protection de la confidentialité de l'information. Les Lignes directrices pour la mise en oeuvre nationale des principes de l'APEC prévoient que « Le système de protection de la confidentialité d'un État membre devrait comprendre un éventail approprié de moyens pour répondre aux violations de la confidentialité."[62] Le document comporte également en annexe un programme de travail futur qui stipule notamment que :

> « Les économies membres doivent coopérer en vue d'offrir des moyens de réparation contre des violations de confidentialité qui présentent une dimension transfrontière. Dans ce but, les économies membres s'attacheront à élaborer des mécanismes de coopération entre les organismes d'investigation et de mise en application de la confidentialité des données des économies membres. »

Pour promouvoir ce programme de travail, le sous-groupe sur la confidentialité de l'APEC oeuvre à l'élaboration de règles en matière de confidentialité transfrontière ainsi qu'au développement des échanges de l'information et de la coopération entre autorités de protection de la vie privée en matière d'investigation et d'exécution.

Autres accords de coopération sur la protection de la vie privée

Parmi les autres mécanismes de coopération figure l'Accord de la sphère de sécurité (Safe Harbor) entre les États Unis et l'UE,[63] un Protocole d'Accord de 2005 entre l'Autorité espagnole de protection des données et la FTC américaine (sur le spam)[64], le sous-groupe sur la confidentialité de l'APEC et les accords Eurojust, Schengen, Europol et le système d'information des douanes (SID) pour la coopération européenne dans le domaine de l'application de la loi.

Il existe de nombreux accords de coopération moins formels mais importants (qui ne sont pas principalement axés sur l'exécution). La Conférence internationale des commissaires à la protection des données et à la vie privée se réunit annuellement pour aborder une vaste gamme de sujets touchant à la vie privée. Le Groupe de travail international sur la protection des données dans les télécommunications (parfois appelé groupe de Berlin) se réunit habituellement deux fois par année sur des sujets divers. L'Australie, la Corée, la Nouvelle Zélande et Hong Kong, Chine se rencontre tous les deux ans sous l'égide du Forum des autorités de protection de la vie privée d'Asie Pacifique (anciennement PANZA+). En 2003 l'Autorité de protection des données espagnole a fondé le Réseau ibéro-américain de protection des données (IDPN) pour appuyer à titre de forum consultatif les efforts nationaux de protection des données en Amérique latine.[65] On peut également mentionner le Case Handling Workshop de l'UE qui se réunit deux fois par an et le mécanisme de demande d'assistance auprès des autres autorités et d'échange d'information via le site Internet CIRCA de la Commission européenne. D'autres mécanismes de coopération existent sous la forme de réunions de groupes régionaux traitant non seulement des politiques générales mais aussi de thèmes spécifiques : par exemple la Conférence annuelle de printemps des autorités européennes de protection des données, les réunions semestrielles des Îles Britanniques, les réunions des pays francophones et les réunions des autorités scandinaves.

D. Les instruments de coopération de l'OCDE sur la protection des consommateurs et le spam

Beaucoup de choses pourraient être apprises du travail sur la coopération d'application des lois dans d'autres domaines, qu'ils soient civils, administratifs ou criminels[66]. L'OCDE a déjà mené une cation pour promouvoir la coopération pour l'application transfrontière de la législation dans deux domaines qui ont un rapport avec les travaux sur la coopération concernant la vie privée, à savoir la protection des consommateurs et le spam[67]. Dans ces deux domaines, l'OCDE a mis en place des instruments de coopération qui visent à faire face aux défis les plus courants en matière d'application transfrontière :

- Les restrictions sur les compétences des autorités d'application.
- Les limitations en matière de collecte et d'échange d'informations.
- Les possibilités limitées de faire appliquer les décisions à l'extérieur des frontières nationales; et
- Les différences au niveau des priorités d'exécution des autorités d'application.[68]

Ces deux instruments énoncent des principes fondamentaux, mais ils laissent aux pays membres et à leurs autorités d'application respectives la responsabilité de la mise en œuvre. D'après ces instruments, les réseaux existants et les accords bilatéraux de coopération continueront à fournir une aide dans les litiges transfrontières.

Lignes directrices sur la fraude transfrontière

En 2003, les pays membres de l'OCDE ont adopté de nouvelles Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses (« Lignes directrices sur la fraude transfrontière »).[69] Ces Lignes directrices reconnaissent qu'une amélioration de la coopération internationale commence par la mise en place de systèmes nationaux

efficaces qui dotent les autorités d'application des pouvoirs et des outils nécessaires pour faire enquête, recueillir et échanger des éléments de preuve et mettre un terme aux conduites répréhensibles.

Les Lignes directrices sur la fraude transfrontière énoncent des principes en matière de coopération internationale, en mettant l'accent sur la notification, l'échange d'information, l'assistance en matière d'enquête, la confidentialité et la compétence des autorités d'application. Les pays membres sont incités à établir un point de contact unique afin de faciliter la coopération internationale. Les Lignes directrices soulignent également l'importante contribution pouvant être apportée par le secteur privé pour le succès de l'application transfrontière. Enfin, les Lignes directrices appellent à la poursuite des travaux sur certains des aspects les plus complexes de l'application transfrontière, y compris les voies de recours, le gel des avoirs et l'exécution et la reconnaissance mutuelle des décisions judiciaires.

Pour certains pays, la mise en oeuvre des Lignes directrices sur la fraude transfrontière a exigé des modifications législatives ; ainsi certains pays ont vu la création de nouvelles autorités.[70] Pour d'autres pays, jusqu'à présent, les efforts d'application ont surtout porté sur les aspects opérationnels. Pour la quasi totalité des pays, la de modernisation des autorités d'application pour faire face aux réalités du marché mondialisé sera un processus de longue haleine.

Recommandation relative à la lutte contre le spam

En s'appuyant sur les Lignes directrices sur la fraude transfrontière, le Conseil de l'OCDE a adopté le 7 avril 2006 une *Recommandation relative à la coopération transfrontière dans l'application des législations contre le spam* (« Recommandation contre le Spam »).[71] Le problème de l'application de la législation contre le spam souligne la nécessité de coopération à l'échelle mondiale pour résoudre les nombreux défis qui se posent en matière de collecte et d'échange d'informations, identifier les priorités en matière d'application et élaborer des cadres d'application internationaux performants.

Bien que son objectif soit le renforcement de la coopération, la Recommandation souligne que la décision ultime de fournir ou non de l'assistance dans une affaire donnée appartient à l'autorité d'application saisie de la requête. Avant de présenter une demande d'assistance en vertu de la Recommandation les autorités d'application sont incitées à mener une enquête préliminaire, à essayer d'établir un ordre de priorités et à faire usage des ressources communes existantes.

La Recommandation contre le spam a une signification particulière dans le cadre de la coopération relative à l'application de la législation sur la vie privée parce que de nombreux pays membres de l'OCDE ont chargé leurs autorités d'application de la législation sur la vie privée également de l'application de la législation contre le spam et celles-ci entrent, en conséquence, dans le champ de la Recommandation.

CONCLUSION

Comme le soulignait un responsable de l'application de la législation sur la vie privée lors d'un colloque de l'APEC en 2004, la coopération en matière d'application « semble être instinctivement une bonne chose ».[72] Nous disposons désormais d'éléments supplémentaires en faveur d'une coopération efficace. Les réseaux d'information et de communications ont augmenté en taille et en capacité, les efficiences professionnelles et opérationnelles qu'ils entraînent ont été accompagnées de risques croissants au niveau de la vie privée. Atténuer ces risques tout en assurant la confiance nécessaire dans une économie mondiale et dépendante de la libre circulation des informations demande une forte coopération pour l'application transfrontière de la législation relative à la vie privée. Le besoin d'une meilleure coopération en matière d'application – identifié au départ dans les lignes directrices de 1980 – est maintenant devenu une priorité au sein et à l'extérieur de l'OCDE.

Le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée prévoit de poursuivre ses travaux sur les sujets abordés dans le présent rapport, en vue de renforcer la capacité des autorités à oeuvrer ensemble dans les affaires transfrontières. Les conclusions du présent rapport font apparaître de nombreux sujets possibles pour des études futures dont notamment :

- L'examen des approches en matière de traitement et de classification des plaintes transfrontières.
- La recherche de priorités communes pour la coopération en matière d'application.
- L'amélioration de la coopération entre les autorités en ce qui concerne les notifications, l'échange d'informations et l'assistance en matière d'enquête.
- L'examen de la pertinence des sanctions et recours dont disposent les autorités d'application de la législation sur la vie privée dans le contexte de litiges transfrontières.
- L'amélioration des perspectives de reconnaissance des jugements et d'exécution des ordonnances au plan international prononçant des compensations financières en faveur des individus victimes de violation de la vie privée.[73]
- L'examen des méthodes informelles de coopération internationale – souvent par le biais de réseaux régionaux – permettant l'échange d'informations sur les questions d'actualité et les meilleures pratiques.
- L'évaluation du besoin d'outils pratiques, tels que des listes de contacts, des formulaires de demande d'assistance auprès d'autorités étrangères, des formulaires de plaintes transfrontières, des protocoles communs de communication de résultats, etc.
- L'établissement d'un ensemble d'indicateurs plus complets et plus fiables sur l'ampleur des problèmes relatifs à la protection de la vie privée dans un cadre transfrontière.

Pratiquement tous les pays de l'OCDE ont mis en place des autorités d'application des lois chargées de l'application de la législation relative à la vie privée. Une attention accrue des questions décrites ci-dessus pourra aider à s'assurer que ces autorités peuvent exercer leur responsabilité avec succès quand les défis transfrontières surviendront.

NOTES

1 Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (23 septembre 1980), OCDE, Paris, ISBN 92-64-19719-2.

2 Conseil de l'Europe (CoE) (1981). Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, Conseil de l'Europe. Série des traités européens N° 108.

3 Assemblée générale des Nations Unies, Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés le 14 décembre 1990.

4 Voir, www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html

5 Voir OCDE, Broadband Statistics, Décembre 2005, disponible à : www.oecd.org/document/39/0,2340,en_2649_37441_36459431_1_1_1_37441,00.html

6 TeleGeography Research, "Internation Internet Statistics" (2005) www.itu.int/dms_pub/itu-d/md/02/isap2b.1.1/c/D02-ISAP2B.1.1-C-0025!!PDF-E.pdf

7 OECD, Internet Traffic Exchange: Market Developments and Measurement of Growth (2006) p.13, www.oecd.org/dataoecd/25/54/36462170.pdf

8 Colin Bennett and Charles Raab, *The Governance of Privacy* (MIT, Cambridge Mass 1996) p. xvi.

9 Christopher Kuner, *European Data Privacy Law and Online Business* (Oxford U. Press 2003), p. ix.

10 U.S. Dept. of Commerce, "Safe Harbor Workbook," available at: www.export.gov/safeharbor/sh_workbook.html

11 Suivant une étude, 61 % des adolescents donnent leurs coordonnées sur leurs blogs en communiquant leur adresse e-mail (44%), leur pseudo de messagerie instantanée (44%) ou un lien vers leur page personnelle (30%). Ils sont 59 % à donner leur localisation par le nom soit de la ville soit de la région. Parmi les adolescents qui tiennent un blog 39% donnent leur date de naissance, et 20% divulguent leur nom au complet. Voir David Huffaker, "Teen Blogs Exposed: The Private Lives of Teens Made Public" (2006), disponible sur www.soc.northwestern.edu/gradstudents/huffaker/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf.

12 Voir *par exemple* Elliot Maxwell, "Some Reflections on the Future: Dipping a Toe in the Datastream"; Présentation durant le "Foresight Forum on Radio Frequency Identification (RFID)" de l'OECD. Applications and Public Policy Considerations, Paris, 5 Oct. 2005, disponible à : www.oecd.org/dataoecd/60/20/35466861.pdf

13 The Tipping Point, Malcolm Gladwell, 2000-2002, Back Bay Books.

14 Une majorité croissante des 5 257 ménages canadiens et américains sondés indique que des inquiétudes quant à la vie privée affectent leur comportement en ligne. Voir, Forester Research, "The Consumer Privacy Bluff" (13 décembre 2005).

15 Voir, Harris Interactive, "Global Consumer Perceptions towards Data Security," (January 2006), disponible à : http://corporate.visa.com/av/pdf/DataSecurityResearch.pdf

16 Voir, IPSOS "Interest in Online Banking Flattens", (6 September 2005) disponible à : www.ipsos-na.com/news/pressrelease.cfm?id=2765

17 Voir, John Leydon, "Consumers punish firms over data security breaches" (15 November 2005) reporting on a study by the Ponemon Institute, disponible à : www.theregister.co.uk/2005/11/15/data_security_breach_survey/

18 Voir, Peter Swire, "The Internet and the Future of Consumer Protection," (24 July 2006) disponible sur : www.americanprogress.org/atf/cf/%7BE9245FE4-9A2B-43C7-A521-5D6FF2E06E03%7D/SWIRE_CONSUMER_PROTECTION_REPORT.PDF

19 Cette action judiciaire a été intentée par l'Attorney General de l'État de New York, qui a obtenu que la société verse 1.1 million d'USD. Voir, www.oag.state.ny.us/press/2006/mar/mar23a_06.html

20 Voir, BNA, "Japan Sees Jump in Data Breach Reports in FY '05," Vol.5 No.28 (10 July 06). Bien que les chiffres pour l'année fiscale 2005 aient triplé par rapport à ceux indiqués pour l'année 2004, ce bond pourrait être dû en partie à un changement dans la législation japonaise qui a résulté à une déclaration obligatoire.

21 Plusieurs États des États-Unis ont promulgué des dispositions qui rendent obligatoire la notification aux particuliers de violation de la sécurité des données dans certaines circonstances. De telles dispositions sont moins fréquentes en Europe et ailleurs. Voir BNA, "Security Breaches: Legal Requirements in Europe"; (Juin 06), Vol. 6, N° 6, p. 26.

22 、 Voir, www.ftc.gov/opa/2006/02/cardsystems_r.htm

23 Voir, www.meti.go.jppolicy/commerce_distribution/kouhyouyou.html

24 La FTC américaine a obtenu une amende de USD 10 millions et USD 5 million en dédommagement des consommateurs. Voir, www.ftc.gov/opa/2006/01/choicepoint.htm

25 Une liste de cas de violation de la sécurité des données rapportés par des organisations américaines se trouve sur www.privacyrights.org/ar/ChronDataBreaches.htm

26 La récente enquête sur la criminalité informatique du CSI/FBI conclut que la plupart des organisations s'inquiètent encore de la publicité négative causée par l'annonce d'intrusions. Même dans le cadre d'une enquête anonyme, seule la moitié des 616 sociétés américaines interrogées était disposée à communiquer les pertes financières totales engendrées par les violations de sécurité. Voir, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

27 Voir, www.hummingbird.com/press/2006/texas_guaranteed.html

28 Voir, www.thisismoney.co.uk/saving-and-banking/article.html?in_article_id=401667&in_page_id=7

29 Voir, Associated Press, "Equifax laptop with employee data stolen" (20 June 2006) disponible sur : www.msnbc.msn.com/id/13437723/

30 Voir, BNA, Privacy and Security Law Report, Vol. 5, No. 27 (3 July 2006) p. 948.

31 Voir, www.montereyherald.com/mld/montereyherald/news/15133805.htm

[32] L'armée américaine a récemment annoncé que les données à caractère personnel comprenant le nom complet et le numéro de sécurité sociale de 100 000 militaires avait été rendues accessibles en ligne par inadvertance sur un site Internet officiel du gouvernement américain. Voir, www.news.navy.mil/search/display.asp?story_id=24568

[33] Voir www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/Cross-BorderCY-2005.pdf

[34] Inger-Anne Ravlum, "Pinning our faith on Big Brother" (2005). Voir, www.toi.no/article17922-29.html

[35] Voir, ICO Communications and External Relations Strategy, Three year plan 2006-2009, p. 4 disponible à : www.ico.gov.uk/cms/DocumentUploads/Communications_and_External_Relations_Strategy_2006-09_full_version.

[36] Voir Bennet and Rabb (2006), p. 263 compte-rendu des études sur le Canada et l'Australie.

[37] Voir OCDE, « Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandations de l'OCDE » (2006) disponible à : http://olishdweb.oecd.org/Hyperdoc/2006/07/24/JT03212215doc/index.aspx

[38] Déclaration sur la protection de la vie privée sur les réseaux internationaux faite par les Ministres à la Conférence "A Borderless World: Realising the Potential of Global Electronic Commerce", 7-9 Octobre 1998, Ottawa, Canada.

[39] OCDE, « Protection de la vie privée en ligne : Orientations politiques et pratiques de l'OCDE », p. 29-31 (2003). Disponible à : www.oecd.org/document/49/0,2340,fr_2649_34255_19216241_1_1_1_1,00.html

[40] Voir, www.oecd-antispam.org

[41] www.oecd.org/sti/crossborderfraud

[42] Voir, « Protection de la vie privée en ligne », OCDE, p. 19.

[43] Voir par exemple, le rapport et les documents préparés pour la conférence en novembre 2005 par le *United Kingdom Information Commissioner*, disponible à : www.ico.gov.uk/eventual.aspx?id=16537

[44] Dans cette section du rapport, le nombre des réponses a été calculé en utilisant uniquement les données du Commissariat fédéral allemand. Des observations distinctes sont faites sur la position des autorités des États fédérés allemands.

[45] Voir par exemple l'Article 14 de la Convention basé sur l'Article K.3 du Traité de l'Union européenne, sur l'établissement de l'Office européen de police (Europol) [Journal officiel C 316 du 27.11.1995].

[46] Premier rapport sur la mise en œuvre de la Directive sur la protection des données, COM(2003)265 final, p. 20.

[47] Kuner, (2003) p. 37.

[48] Voir, www.ftc.gov/opa/2006/05/phonerecords.htm

[49] Le Groupe de travail sur la Protection des Particuliers concernant le traitement de données à caractère personnel a été mis en place sous l'Article 29 de la Directive de l'Union Européenne sur la protection des données, 95/46/EC.

[50] Voir Groupe de travail Art. 29, « Avis 1/2005 sur le niveau de protection assuré au Canada à la transmission des dossiers passagers et des informations anticipées sur les voyageurs par les compagnies aériennes » (2005) consultable à : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp103_fr.pdf

[51] Voir Groupe de travail Art. 29, « Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP) », consultable à : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_fr.pdf

[52] Voir Groupe de travail Art. 29, « Premières orientations du document de travail du groupe de travail Article 29 concernant les services d'authentification en ligne ». (2002) consultable à : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp60_fr.pdf

[53] Voir, www.ftc.gov/opa/2002/08/microsoft.htm

[54] Pour un débat sur ces questions dans le contexte des décisions sur la protection des consommateurs, voir OCDE, « Rapport général sur le règlement des litiges avec les consommateurs et la réparation sur le marché mondial » (2005) pp. 39-43, disponible sur : http://www.oecd.org/dataoecd/54/49/35201271.pdf

[55] Au Japon le Cabinet du Premier ministre pourrait sans doute fournir des informations sur les questions touchant le secteur privé.

[56] Voir note 2 supra.

[57] Conseil de l'Europe, Convention de sauvegarde des Droits de l'homme et des libertés fondamentales, Série 5 du traité européen de Strasbourg, 1950.

[58] Voir note 3 supra.

[59] Premier rapport de la Commission Européenne sur la mise en œuvre de la Directive relative à la protection des données IP/03/697 Date: 16/05/2000.

[60] Déclaration du Groupe de travail Article 29 concernant la mise en application 12067/04/FR WP 101.

[61] Voir, www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.tml

[62] Voir, http://203.127.220.112/content/apec/apec_groups/som_special_task_groups/electronic_commerce.downloadlinks.0004.LinkURL.Download.ver5.1.9

[63] Voir, www.export.gov/safeharbor/index.html. A ce jour, l'organe établi par les autorités européennes de protection des données pour examiner les plaintes des individus en vertu de l'Accord de la sphère de sécurité avec les États-Unis n'a été saisi d'aucun cas.

[64] Voir, www.ftc.gov/os/2005/02/050224memounderstanding.pdf

[65] www.agpd.es/index.php?idSeccion=349

[66] Par exemple, le recent travail dans le domaine de la cybercriminalité soulève des questions similaires concernant les problèmes de partage d'information, voir par exemple, le Conseil de l'Europe, Convention sur la cybercriminalité, disponible à : http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm ou l'Union Européenne : « Décision cadre 2005/222/JAI du Conseil », disponible à : http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2005/l_069/l_06920050316fr00670071.pdf

[67] L'OCDE a aussi joué un rôle actif dans la promotion de la coopération dans le domaine de l'application de la legislation sur la concurrence. Voir, *Recommandation révisée du Conseil sur la coopération entre pays membres dans le domaine des pratiques anticoncurrentielles affectant les échanges internationaux*, C(95)130/FINAL, disponible à : www.oecd.org/concurrence.

[68] OCDE, « Rapport sur l'application des lois antispam, » DSTI/CP/ICCP/SPAM(2004)3/FINAL, p.4.

[69] Voir, www.oecd.org/sti/crossborderfraud

[70] OCDE, « Rapport sur la mise en œuvre des Lignes directrices de 2003 régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses » (2006), consultable à : www.oecd.org/dataoecd/2/5/37133090.pdf

[71] Voir, www.oecd-antispam.org/article.php3?id_article=237v

[72] Blair Stewart "Cross Border Co-operation on Enforcement Matters" Colloque de l'Apec sur les mécanismes de mise en œuvre de la confidentialité, Santiago, Chili 23-24 Février 2004.

[73] Pour un débat sur ces questions, voir OCDE, « Le règlement des litiges avec les consommateurs et la réparation sur le marché mondial » (2005) pp. 39-41. www.oecd.org/dataoecd/26/61/36456184.pdf

ANNEXE A. TABULATION OF THE RESPONSES TO THE QUESTIONNAIRE

Questions:	Enforcement Authority				Complaint Handling							Investigation/Audits/Inspection										
	Date	Budget M Euros	Staff	Enforcement Staff	Receive complaints	Citizen	Resident	Mail	Phone	On-line	Inv. Duty	Own motion	Testimony	Documents	3rd Parties	Enter Premises	Stop Processing	On-site Audits	Grounds	Inform	Consent	Other
AUSTRALIA	1988	2,52	39	39	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y
AUSTRIA	1980		20	5	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
BELGIUM	1992	4,61	59	25	Y	N	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
CANADA	1983		86	30	Y	N	N	Y	N	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N
CZECH REPUBLIC	2000	3,2	80	50	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
DENMARK	1979	2	37	31	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y
FRANCE	1978	7	102	102	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y
GERMANY	1978	3,69	69	56	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
HUNGARY	1995	1,3	52	31	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y
ICELAND	2001	0,5	8	6	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N
ITALY	1997	16,5	105	5	Y	N	N	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
JAPAN - Private Sector[1]	2003	0,7	44	44	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	N	Y	N	N	N	N	N
KOREA - MIC	1948		441	8	Y	N	N	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N
KOREA - KISA	1996			10	Y	N	N	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N
NETHERLANDS - CBP	1989	5,46	71	12	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
NETHERLANDS - OPTA	1997	18	140	8	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
NEW ZEALAND	1991	1,4	31	12	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N	Y	Y	Y
NORWAY	1980	2,9	31	24	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
POLAND	1998	2,7	116	81	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
SPAIN	1993	9,45	115	77	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
SWITZERLAND	1993		19,6	19,6	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
UNITED KINGDOM	1984				Y	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N
UNITED STATES - FTC	1914	211 USD	varies	varies	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N
ALBANIA (Non-member)	2000	0,575	45	2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N

1. The budget figure is only for the cabinet office (excludes competent ministers) and the staff figure is for both cabinet office and competent ministers.

Questions:	Sanctions, remedies, etc. by the Authority														Sanctions through legal system					
	Mediation	Binding arbitration	Legal Assistance	Legal decision	Binding decision	Publicity	Warning/ reprimand	Negotiate fine, etc	Legal order	Compensation	Court Injunctions	Penalties	Criminal case	Other	Orders	Compensation	Civil penalties	Criminal fines	Jail	Other
AUSTRALIA	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	N	N	Y	Y	N	Y	Y	N
AUSTRIA	Y	N	Y	Y	Y	N	Y	N	Y	N	N	N	Y	N	Y	Y	N	Y	Y	N
BELGIUM	Y	N	N	N	N	Y	N	N	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
CANADA	Y	N	Y	Y	N	Y	Y	N	N	N	Y	N	N	N	Y	Y	Y	Y	N	N
CZECH REPUBLIC	N	Y	N	Y	Y	Y	N	Y	Y	N	N	Y	Y	N	N	Y	N	Y	Y	N
DENMARK	N	N	N	Y	Y	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
FRANCE	N	N	N	Y	Y	Y	Y	N	Y		N	Y	N	N	Y	Y	Y	Y	Y	N
GERMANY	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N
HUNGARY	Y	N	N	Y	Y	Y	Y	N	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	N
ICELAND	N	N	N	Y	Y	Y	N	N	Y	N	N	N	N	Y	N	Y	Y	Y	Y	N
ITALY	N	N	N	Y	Y	Y	Y	N	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N
JAPAN - Private Sector	N	N	N	Y	N	Y	Y	N	Y	N	N	Y	N	N	N	N	N	Y	Y	N
KOREA - MIC	N	N	N	Y	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	Y	Y	Y	N
KOREA - KISA	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	N
NETHERLANDS - CBP	Y	N	Y	Y	N	Y	Y	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	N
NETHERLANDS - OPTA	N	N	N	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	Y	N	Y	Y	N
NEW ZEALAND	Y	N	Y	Y	N	Y	N	N	N	N	Y	Y	N	Y	Y	Y	N	N	N	Y
NORWAY	Y	N	N	Y	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N
POLAND	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	Y	Y	Y	Y	N
SPAIN	N	N	N	Y	Y	Y	N	N	Y	N	N	Y	N	N	Y	N	Y	Y	N	N
SWITZERLAND	N	N	N	Y	N	Y	N	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	N	N
UNITED KINGDOM	N	N	N	Y	N	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	N	Y	N	N
UNITED STATES - FTC	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	N	N	N
ALBANIA (Non-member)	Y	N	N	Y	Y	Y	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	N

Questions:	Cross-border Aspects							Obstacles to cross-border co-operation					
	Existing arrangements	Could have Contact Point	Enforcement Priorities	Against foreign controller	Against domestic controller	Notify foreign Authorities	Share info abroad	Lack of legal powers	Legal incompatibilities	Limits on info sharing	Resource limitations	Language barriers	Other
AUSTRALIA	Y	Y	N	N	Y	Y	Y	Y	Y	Y	N	Y	N
AUSTRIA	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N
BELGIUM	N	Y	N	N	Y	Y	Y	Y	Y	N	Y	N	N
CANADA	N	Y	N	Y	N	N	N	Y	N	Y	N	N	Y
CZECH REPUBLIC	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
DENMARK	Y	Y	N	Y	Y	Y	Y	?	?	?	?	?	
FRANCE	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
GERMANY	N	Y	N	N	Y	N	N	Y	N	Y	Y	N	N
HUNGARY	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
ICELAND	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	Y
ITALY	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
JAPAN - Private Sector	N	N	N	N	Y	N	N						
KOREA - MIC	N	Y	Y	N	N	N	Y	Y	Y	N	N	N	N
KOREA - KISA	Y	Y	Y	N	N	N	Y	Y	Y	Y	N	N	
NETHERLANDS - CBP	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N
NETHERLANDS - OPTA	Y	?	Y	N	Y	Y	Y	Y	Y	Y	Y	N	
NEW ZEALAND	Y	Y	Y	?	Y	Y	?	Y	Y	Y	Y	Y	
NORWAY	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	
POLAND	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	
SPAIN	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
SWITZERLAND	N	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N	
UNITED KINGDOM	Y	Y	Y	Y	Y	Y	Y	?	?	N	N	N	
UNITED STATES - FTC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	
ALBANIA (Non-member)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N

ANNEXE B. PRIVACY LAWS AND ENFORCEMENT AUTHORITIES OUTSIDE THE OECD

What follows below is a short overview of the situation outside OECD.[1] While the variety in approaches to privacy within the OECD is significant, it is even greater in non-member economies. There are a number of economies outside the OECD that have a privacy law and enforcement authority. A number of others jurisdiction are currently in the process of developing or approving legislation. For example proposed legislation in South Africa would establish a data privacy of general application and create a new body to enforce the law, while India is considering amending it s Information Technology Act to require improved data security.

Europe

Among the European countries that are not part of the OECD, a significant number have privacy laws, including: Albania,[2] Bosnia and Herzegovina,[3] Bulgaria,[4] Croatia,[5] Cyprus,[6] Estonia,[7] Gibraltar[8], Latvia,[9] Liechtenstein,[10] Lithuania,[11] Malta,[12] Monaco,[13] Romania,[14] Serbia,[15] and Slovenia.[16] Here the influence of the European Union and the Council of Europe has been substantial.

Asia Pacific

Non-members in the Asia-Pacific region with privacy laws include Hong Kong, China; Chinese Taipei; and Thailand.[17] The power of the Hong Kong, China authority[18] to investigate overseas breaches by local companies is uncertain. It would appear that their law would not allow them to share information with a body in another jurisdiction. On the other hand, the law in Chinese Taipei has limited coverage but allows the various sectoral enforcement bodies to restrict export of data in certain circumstances. Thailand has a law that includes principles and mechanisms to protect privacy of people related to personal information controlled or kept within state agencies or state enterprises. It is enforced by the Office of the Information Commissioner.[19]

Other countries in the region have privacy provisions inserted in other laws (for example, cybercrime laws) with limited means of enforcement. These include China, Indonesia, Philippines and Vietnam. A number of these countries are moving towards having more comprehensive privacy law.

Latin America

In Latin America, privacy rights have developed from the concept of "habeas data," which permits individuals to know what information is archived about them by the government, and in some cases the private sectior.[20]Argentina established a comprehensive data protection law in with an independent enforcement authority.[21] Chile's constitution recognises a general right to privacy and it has comprehensive legislation -- the Law for the Protection of Private Life -- which regulates the processing of personal data in the public and private sectors, including human resources data. There is no independent data protection authority, with enforcement by means of individuals bringing private actions in the courts. Paraguay established a data protection law in 2000.[22]

Other Regions

Israel has a Data Protection Inspector and Registrar of Data Bases. Burkina Faso also has general data protection law.

NOTES ANNEXE B.

[1] Member states of the Council of Europe and APEC economies were invited to participate in the work, including by completing the Questionnaire. Only one reply was received, that of Albania which has been incorporated into the broader analysis.

[2] The characteristics of the Albanian system have been incorporated in the body of this report, based on its response to the Questionnaire. An informal translation of the Albanian law is available here: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/AlbaniaProtectionPersonalData.asp#TopOfPage

[3] See, www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/Bosnia&Herz.Data%20Protection%20eng%20received%20080402.asp#TopOfPage

[4] See, www.ceecprivacy.org/main.php?s=2&k=bulgaria

[5] See, www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/NATIONAlLAWS-EN.asp#TopOfPage

[6] For an unofficial translation, see www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/Cyprus%20-%20DP%20Law.asp#TopOfPage.

[7] See, www.dp.gov.ee/index.php?id=14

[8] The law is available at: www.gra.gi/legis/DATA%20PROTECTION%20ORDINANCE.pdf

[9] See, www.dvi.gov.lv

[10] See, www.sds.llv.li

[11] See, www.ada.lt/

[12] The web site of the Data Protection Commissioner of Malta is here: www.dataprotection.gov.mt/

[13] See, www.ccin.mc/

[14] See, www.avp.ro

[15] See, www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/FRY%20DPL.asp#TopOfPage

[16] See, www.ip-rs.si/

[17] The Web site of the Office of the Official Information Commission is here: www.oic.thaigov.go.th/content_eng/default_eng.asp

[18] See, www.pco.org.hk/

[19] www.oic.thaigov.go.th/

[20] See, Pegg Eisenhauer, "Developments in Latin America Privacy Laws" in BNA Privacy and Security Law Report, Vol. 5, No. 15 (10 April 2006), pp521.

[21] See, www2.jus.gov.ar/dnpdp/

[22] www.alston.com/abResourceCenter/docs/ParaguayPrivateInfo.pdf

ANNEXE C. DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN (extrait)

CHAPITRE VI - AUTORITÉ DE CONTRôLE ET GROUPE DE PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT DES DONNÉES A CARACTèRE PERSONNEL

Article 28 - Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment :

- De pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle.
- De pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en oeuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction des données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques.
- Du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre sont elle relève, les pouvoirs dont elle est investi conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les États membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

Article 29 - Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé « groupe ».

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission.

Article 30

1. Le groupe a pour mission :

a) d'examiner toute question portant sur la mise en oeuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en oeuvre homogène.

b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers.

c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés.

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

2. Si le groupe constate que de sérieuses divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des États membres, il en informe la Commission.

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté.

4. Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.

5. La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

ANNEX D. CONVENTION 108 DU CONSEIL DE L'EUROPE (extrait)
Chapitre IV – Entraide, Article 13 – Coopération entre les parties

1. Les Parties s'engagent à s'accorder mutuellement assistance pour la mise en œuvre de la présente Convention.

2. A cette fin :
   a. chaque Partie désigne une ou plusieurs autorités dont elle communique la dénomination et l'adresse au Secrétaire Général du Conseil de l'Europe;
   b. chaque Partie qui a désigné plusieurs autorités indique dans la communication visée à l'alinéa précédent la compétence de chacune de ces autorités.

3. Une autorité désignée par une Partie, à la demande d'une autorité désignée par une autre Partie:
   a. fournira des informations sur son droit et sur sa pratique administrative en matière de protection des données;
   b. prendra, conformément à son droit interne et aux seules fins de la protection de la vie privée, toutes mesures appropriées pour fournir des informations de fait concernant un traitement automatisé déterminé effectué sur son territoire à l'exception toutefois des données à caractère personnel faisant l'objet de ce traitement.

Article 14 – Assistance aux personnes concernées ayant leur résidence à l'étranger

1. Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention.

2. Si une telle personne réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie.

3. La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment:
   a. le nom, l'adresse et tous autres éléments pertinents d'identification concernant le requérant;
   b. le fichier automatisé de données à caractère personnel auquel la demande se réfère ou le maître de ce fichier;
   c. le but de la demande.

Article 15 – Garanties concernant l'assistance fournie par les autorités désignées

1. Une autorité désignée par une Partie qui a reçu des informations d'une autorité désignée par une autre Partie, soit à l'appui d'une demande d'assistance, soit en réponse à une demande d'assistance qu'elle a formulée elle-même, ne pourra faire usage de ces informations à des fins autres que celles spécifiées dans la demande d'assistance.

2. Chaque Partie veillera à ce que les personnes appartenant ou agissant au nom de l'autorité désignée soient liées par des obligations appropriées de secret ou de confidentialité à l'égard de ces informations.

3. En aucun cas, une autorité désignée ne sera autorisée à faire, aux termes de l'article 14, paragraphe 2, une demande d'assistance au nom d'une personne concernée résidant à l'étranger, de sa propre initiative et sans le consentement exprès de cette personne.