

janvier 2003

**INVENTAIRE DES INSTRUMENTS ET DES MÉCANISMES DE NATURE
À CONTRIBUER A LA MISE EN OEUVRE ET AU RESPECT SUR LES RÉSEAUX
MONDIAUX DES LIGNES DIRECTRICES DE L'OCDE SUR LA PROTECTION
DE LA VIE PRIVÉE**

L'inventaire ci-joint a été préparé pour faire le point des instruments et mécanismes (notamment loi, autoréglementation, contrats et technologies) de nature à contribuer à la mise en œuvre et au respect sur les réseaux mondiaux des Lignes directrices de l'OCDE sur la protection de la vie privée. L'objectif de cette étude était d'identifier un éventail d'outils juridiques et de politiques technologiques permettant d'assurer une protection sans faille, ou du moins efficace, de la vie privée.

Chapitre 6

INVENTAIRE DES INSTRUMENTS ET DES MÉCANISMES DE NATURE À CONTRIBUER A LA MISE EN OEUVRE ET AU RESPECT SUR LES RÉSEAUX MONDIAUX DES LIGNES DIRECTRICES DE L'OCDE SUR LA PROTECTION DE LA VIE PRIVÉE¹

Contexte

Afin de contribuer à construire un environnement de confiance pour le développement du commerce électronique et eu égard à ses travaux en cours dans le domaine de l'infrastructure mondiale de l'information et de la société mondiale de l'information, ainsi qu'à sa connaissance acquise lors de l'élaboration des Lignes directrices de l'OCDE sur la protection de la vie privée et à son expérience renouvelée des questions liées à la protection de la vie privée, l'OCDE a décidé en octobre 1997 d'examiner les diverses solutions susceptibles de faciliter la mise en œuvre des principes de protection de la vie privée dans le contexte des réseaux internationaux.

Le rapport intitulé « Mise en œuvre dans l'environnement électronique, et en particulier sur Internet, des Lignes directrices de l'OCDE sur la protection de la vie privée » a proposé que les gouvernements membres de l'OCDE :

- Réaffirment que les Lignes directrices sur la protection de la vie privée sont applicables quelle que soit la technologie utilisée pour collecter et traiter les données.
- Incitent les entreprises qui décident d'étendre leurs activités aux réseaux d'information et de communication à adopter des mesures et des solutions techniques qui garantissent la protection de la vie privée des personnes sur ces réseaux et en particulier sur l'Internet.
- Favorisent l'éducation du public en ce qui concerne la protection de la vie privée et l'utilisation des technologies ; et
- Engagent un dialogue auquel participent les gouvernements, l'industrie et les entreprises, les utilisateurs et les autorités compétentes pour examiner les évolutions, les questions et les politiques dans le domaine de la protection des données à caractère personnel.

Dans ce contexte, un atelier intitulé « Protection de la vie privée dans une société de réseaux mondialisée » a été organisée avec le soutien du Comité consultatif économique et industriel auprès de l'OCDE (BIAC) les 16 et 17 février 1998. Cette Conférence avait pour objet d'examiner les Lignes directrices de l'OCDE dans le contexte des réseaux mondiaux. L'OCDE souhaitait s'appuyer sur les diverses approches adoptées par ses pays membres et aider à identifier les mécanismes et outils technologiques qui pourraient constituer une « passerelle » efficace entre les différentes politiques de protection de la vie privée élaborées par les pays membres. En outre, il a été porté une attention particulière à la nécessité d'encourager le secteur privé à assurer une protection adéquate des données personnelles sur les réseaux mondiaux par une autorégulation effective.

Avec l'objectif d'identifier des solutions pratiques appropriées pouvant être mises en œuvre quelles que soient les différences culturelles, les sessions de la Conférence ont abordé les thèmes suivants :

- Identifier et concilier les besoins du secteur privé et ceux des utilisateurs et des consommateurs et formuler des stratégies efficaces « d'éducation sur la protection de la vie privée ».
- Développer les « technologies protectrices de la vie privée ».
- Mettre en œuvre des mécanismes élaborés par le secteur privé pour assurer le respect des codes de conduite et autres normes de protection de la vie privée ; et
- Adopter des modèles de solutions contractuelles pour les flux transfrontières de données.

A l'issue de la Conférence, les participants ont reconnu qu'une confiance accrue des consommateurs à l'égard de la protection de la vie privée en ligne est une nécessité pour la croissance du commerce électronique d'entreprise à entreprise et que les Lignes directrices de l'OCDE continuent d'offrir un ensemble commun de principes fondamentaux guidant les efforts dans ce domaine. Ils ont affirmé leur détermination à protéger la vie privée des personnes dans un environnement de réseaux en croissance, à la fois pour garantir des droits importants et pour éviter l'interruption des flux transfrontières de données.

La Présidente a noté un large consensus sur le fait que la protection de la vie privée des personnes nécessite les éléments suivants : éducation et transparence ; instruments souples et efficaces ; exploitation maximum des technologies ; force exécutoire et réparation des préjudices.

Elle a également souligné la nécessité de passer en revue les instruments disponibles (loi, autorégulation, contrat et technologie) afin de décrire leur application pratique dans un environnement de réseaux et leur aptitude à répondre aux objectifs des Lignes directrices de l'OCDE (notamment, efficacité, force exécutoire, réparation des préjudices et portée géographique). Une telle étude permettrait d'identifier un éventail de politiques technologiques et d'instruments juridiques et de disposer d'un ensemble de référence pour assurer une protection sans faille, ou du moins efficace, de la vie privée.

Lors de sa réunion de mai 1998, le Groupe de travail sur la sécurité de l'information et la vie privée a décidé que le Secrétariat rédigerait un Inventaire des instruments et des mécanismes de nature à contribuer à la mise en œuvre et au respect sur les réseaux mondiaux des Lignes directrices de l'OCDE sur la protection de la vie privée (« l'Inventaire »), pour examen, commentaires et approbation lors de ses réunions à venir.

Introduction

Le développement des technologies de l'informatique et des réseaux, et en particulier de l'Internet, s'est accompagné d'une migration des activités sociales, commerciales et politiques du monde physique vers l'environnement électronique. L'intégration des réseaux mondiaux à la vie quotidienne soulève des préoccupations concernant la protection de la vie privée. Dans le monde de la technologie numérique et des réseaux mondiaux, les utilisateurs laissent souvent derrière eux des « traces électroniques » durables, c'est-à-dire des relevés numériques des sites où ils sont allés, des choses qu'ils ont regardées, des pensées qu'ils ont exprimées, des messages qu'ils ont envoyés et des biens et services qu'ils ont achetés. En outre, ces données sont généralement détaillées, individualisées et traitables par ordinateur.

Le simple fait de « naviguer » sur le Web peut mettre à la disposition des sites visités une quantité considérable d'informations, même si une bonne partie de ces informations est nécessaire pour permettre les interactions sur Internet et qu'elle est pour l'essentiel conservée sous forme agrégée. Chaque fois que

l'utilisateur accède à une page Web, le « client » (l'ordinateur de l'utilisateur) fournit au « serveur » (l'ordinateur qui héberge le site Web visité) certaines « informations d'en-tête » (Kang, 1995). Ces informations peuvent comprendre² :

- L'adresse Internet Protocol (« IP ») du client³, à partir de laquelle on peut déterminer, au moyen du *Domain Name System*, le nom de domaine et le nom et le lieu de l'organisation qui a fait enregistrer ce nom de domaine.
- Des informations de base sur le logiciel de navigation (navigateur), le système d'exploitation et la plate-forme matérielle utilisée par le client.
- L'heure et la date de la visite.
- L'*Uniform Resource Locator* (URL, adresse sur le Web) de la page Web que l'utilisateur a regardée immédiatement avant d'accéder à la page courante.
- Si un moteur de recherche a servi à trouver le site, la totalité de la requête qui peut être communiquée au serveur ; et
- Suivant le navigateur, l'adresse de courrier électronique de l'utilisateur (si cette option a été choisie dans l'écran de configuration des préférences du navigateur).

En outre, quand un utilisateur navigue sur un site Web, il peut générer des données correspondant à la « succession des clics », telles que les pages visitées, le temps passé sur chaque page et les informations envoyées et reçues.

Souvent, des données à caractère personnel sont aussi divulguées volontairement. Beaucoup de sites commerciaux demandent aux utilisateurs de remplir et de soumettre des formulaires de pages Web pour s'inscrire, s'abonner, adhérer à un groupe de discussion, concourir, faire des suggestions ou effectuer une transaction. Généralement, les données demandées incluent les nom, adresse, numéro de téléphone personnel ou professionnel et adresse de courrier électronique de l'utilisateur. Quelquefois, des données sont aussi collectées sur l'âge, le sexe, la situation matrimoniale, la profession, les revenus et les centres d'intérêt personnels. En outre, les formulaires d'achat demandent habituellement des informations relatives à la carte de crédit du visiteur (type, numéro et date d'expiration). D'autre part, lorsqu'il est demandé au visiteur d'envoyer des informations au site Web par courrier électronique, ce site peut alors (comme n'importe quel destinataire d'un message électronique) trouver l'adresse électronique du visiteur dans l'« en-tête » du message.

Les « cookies »⁴ sont de petits ensembles de données créés par le serveur d'un site Web et placés sur le disque dur de l'utilisateur. Les « cookies » ont été conçus pour aider l'interaction client-serveur et la collecte de données, et le serveur peut y accéder au cours d'une visite en cours ou de visites ultérieures du site Web⁵. Les « cookies » peuvent servir à faciliter la collecte, le regroupement et la réutilisation des données d'en-tête, de succession de clics ou des données fournies volontairement. Cela se fait généralement en attribuant un numéro de code propre à chaque visiteur et en enregistrant ce numéro dans un cookie que le serveur retrouve à chaque visite du site. On peut associer ce numéro de code à l'information qui est ensuite collectée au sujet de l'utilisateur.

Ainsi, en même temps que le développement des réseaux mondiaux et de la technologie numérique est la source de nombreux bienfaits sociaux et économiques, des technologies récentes augmentent le risque que des informations personnelles soient automatiquement générées, collectées, stockées, interconnectées et employées à des fins diverses par des entreprises en ligne ou par des organismes publics, sans que la personne concernée ne le sache ou y consente.

Le présent Inventaire porte sur les divers instruments, pratiques, techniques ou technologies, qui se recouvrent ou se complètent, qui sont en usage ou en cours d'élaboration, et tendent à définir, mettre en œuvre et faire respecter les principes de la protection de la vie privée dans les environnements de réseaux.

L'Inventaire se divise en deux grandes sections. La Section I décrit les instruments internationaux, régionaux et nationaux, législatifs ou d'autorégulation, qui existent ou sont en cours d'élaboration pour la protection des données à caractère personnel et de la vie privée dans les pays membres de l'OCDE. Une attention particulière est portée aux instruments spécifiquement créés pour l'environnement en ligne. Dans la Section II, sont examinés les mécanismes existants ou en cours d'élaboration visant à mettre en œuvre et faire respecter sur les réseaux mondiaux les principes de protection de la vie privée. En outre, sont donnés en Appendice les adresses d'une grande partie des organisations publiques, privées, nationales, régionales ou internationales de la protection de la vie privée mentionnées dans le présent Inventaire.

I. Instruments juridiques et d'autorégulation

Cette Section de l'Inventaire présente les instruments d'orientation internationaux, régionaux ou nationaux, et les institutions compétentes, pour la protection des données à caractère personnel et de la vie privée.

Au niveau international et régional, un certain nombre d'organisations multilatérales (intergouvernementales ou du secteur privé) ont produit, produisent ou ont l'intention de produire des textes et normes visant à promouvoir la protection de la vie privée. Ces organisations servent aussi d'enceintes pour la poursuite de recherches, pour la formulation des politiques et le dialogue entre les gouvernements, les entreprises, les chercheurs et les associations de défense du public. Les instruments créés par le biais de ces organisations ont souvent une grande influence sur les législations nationales et les instruments d'autorégulation concernant la protection de la vie privée.

Au niveau national, dans la plupart des pays, la protection de la vie privée et des données à caractère personnel associe des instruments législatifs, des organismes gouvernementaux et des instruments d'autorégulation de l'industrie. Tous les pays membres de l'OCDE ont, sous une forme ou une autre, une législation qui concerne le traitement des données à caractère personnel. Un certain nombre de pays ont promulgué des lois « horizontales » qui appliquent les principes de la protection des données personnelles de manière généralisée, au secteur public comme au secteur privé. D'autres législations de protection des données sont davantage sectorielles ; elles ne s'appliquent qu'à un secteur particulier (par exemple, les administrations publiques) ou à un type de données particulier (par exemple, données de santé).

La plupart des pays membres de l'OCDE ont aussi créé des autorités centrales de surveillance, couramment appelées en anglais *Data Protection Officer* ou *Privacy Commissioner* (Commissaire à la protection de la vie privée). Les missions et pouvoirs de ces organismes varient d'un pays à l'autre mais comprennent généralement des missions de conseil, d'examen des plaintes et de mise en œuvre d'actions répressives.

Dans certains pays membres de l'OCDE, on considère l'autorégulation comme un moyen souple et efficace d'assurer la protection de la vie privée en ligne, permettant aux mécanismes du marché et aux initiatives de l'industrie d'apporter des solutions innovantes. On peut définir de manière générale les instruments d'autorégulation comme étant les règles élaborées et mises à exécution par les entités auxquelles elles sont destinées à s'appliquer. Des tiers indépendants peuvent jouer un rôle dans la mise en application de l'autorégulation. Toutefois, les autorités publiques peuvent aussi participer à l'élaboration, à la mise en place et à la mise à exécution des codes ou lignes directrices de l'industrie. Les gouvernements peuvent collaborer avec le secteur privé à la formulation de critères garantissant une protection efficace de

la vie privée, que le secteur privé peut ensuite mettre en œuvre par le moyen de codes d'autorégulation. Dans un certain nombre d'autres pays, on considère les codes d'autorégulation comme un moyen de mettre en œuvre une législation de protection de la vie privée dans le contexte d'une branche d'activité particulière⁶, ou comme une aide à l'interprétation des principes généraux de protection de la vie privée. Dans certains pays membres de l'OCDE comme l'Irlande et la Nouvelle-Zélande les codes sectoriels qui reçoivent une approbation officielle peuvent avoir force de loi.

A. Instruments et organisations à l'échelle internationale et régionale

1. Instruments juridiques intergouvernementaux

- a) Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données

Statut

La *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (« Lignes directrices de l'OCDE ») (OCDE, 1980) a été adoptée par le Conseil de l'OCDE le 23 septembre 1980. Les Recommandations du Conseil ne sont pas des instruments ayant force obligatoire mais elles expriment un engagement « politique » de la part des pays membres. Le Conseil a recommandé que « les pays membres tiennent compte dans leur législation interne, des principes concernant la protection de la vie privée et des libertés individuelles exposés dans les lignes directrices », qu'ils « s'efforcent de supprimer ou évitent de créer, au nom de la protection de la vie privée, des obstacles injustifiés aux flux transfrontières de données de caractère personnel » et qu'ils « coopèrent pour mettre en œuvre les Lignes directrices » (OCDE, 1980).

Les principes constituant les Lignes directrices de l'OCDE sont appliqués dans les pays membres et d'autres pays au moyen d'instruments variés.

Portée

Il existe un large consensus sur le fait que les Lignes directrices constituent un ensemble de principes de protection de la vie privée internationalement reconnu, technologiquement neutres, qui a résisté à l'épreuve du temps. Les Lignes directrices s'appliquent à « toute information relative à une personne physique identifiée ou identifiable »⁷, et leur champ couvre les données du secteur public et du secteur privé, tous les supports de traitement informatisé des données relatives aux personnes physiques (des ordinateurs locaux jusqu'aux réseaux aux ramifications mondiales) et tous les types de traitement de données.⁸

Principes de base

Les Lignes directrices de l'OCDE sur la protection de la vie privée énoncent huit principes de base gouvernant le traitement des informations à caractère personnel. Ces « Principes de protection de la vie privée » sont les suivants :

1. **Limitation en matière de collecte** : Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

2. **Qualité des données :** Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.
3. **Spécification des finalités :** Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.
4. **Limitation de l'utilisation :** Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe de « spécification des finalités », si ce n'est : (a) avec le consentement de la personne concernée, ou (b) lorsqu'une règle de droit le permet.
5. **Garanties de sécurité :** Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation des données.
6. **Transparence :** Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques ayant trait aux données à caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données à caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du responsable du fichier et le siège habituel de ses activités.
7. **Participation individuelle :** Toute personne physique devrait avoir le droit : (a) d'obtenir du responsable d'un fichier, ou par d'autres voies, confirmation du fait que le responsable du fichier détient ou non des données la concernant ; (b) de se faire communiquer les données la concernant : dans un délai raisonnable ; moyennant, éventuellement, une redevance modérée ; selon des modalités raisonnables ; et sous une forme qui lui soit aisément intelligible ; (c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et (d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
8. **Responsabilité :** Tout responsable de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Dispositions concernant les flux de données

Les Lignes directrices de l'OCDE tendent à éviter que l'on impose des obstacles inutiles aux flux transfrontières de données⁹. Toutefois, des restrictions légitimes sont admises. Par exemple, un pays membre peut imposer des restrictions au transfert de « certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays membre ne prévoit pas de protection équivalente ».

Dispositions concernant la poursuite de la coopération

Les Lignes directrices de l'OCDE créent un cadre pour la poursuite de la coopération¹⁰ qui consiste notamment à veiller à ce que les procédures applicables aux flux transfrontières de données et à la protection de la vie privée soient simples et compatibles avec celles des autres pays membres, à établir des procédures en vue de faciliter l'échange d'informations et à établir des principes, sur le plan intérieur et

international, pour identifier le droit applicable dans les pays membres en cas de flux transfrontières de données de caractère personnel.

Dispositions concernant la mise en œuvre et l'exécution

Les Lignes directrices appellent les pays membres à mettre en œuvre ces principes sur le plan intérieur en établissant des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée et les données à caractère personnel¹¹. Parmi les moyens permettant de réaliser cet objectif, on peut citer le fait d'adopter une législation nationale appropriée ; d'encourager et soutenir les systèmes d'autorégulation ; de donner aux personnes physiques des moyens raisonnables pour exercer leurs droits ; d'instituer des sanctions et des recours appropriés en cas d'inobservation des mesures mettant en œuvre les principes ; et de veiller à ce que les personnes concernées ne fassent l'objet d'aucune discrimination inéquitable.

Travaux en cours

L'OCDE, par le biais du Comité de la Politique de l'information, de l'informatique et des communications (« Comité PIIC »), continue de travailler dans le domaine de la protection de la vie privée et des données et fournit une enceinte de discussion sur des questions nouvelles telles que les défis que présente l'émergence des réseaux mondiaux¹².

- b) Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Statut

La Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 18 septembre 1980 (« Convention 108 ») (COE, 1980) a été ouverte à la signature par le Comité des Ministres du Conseil de l'Europe le 28 janvier 1981. Depuis lors, elle a été signée par 33 pays et ratifiée par 29 (voir Tableau 6.1)¹³. La Convention 108, à laquelle peuvent accéder tous les États et non pas simplement les États membres du Conseil de l'Europe, est un instrument du droit international ayant force obligatoire.

Portée

La Convention s'applique aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.¹⁴

Principes de base

Les principes de base de la Convention sont similaires à ceux des Lignes directrices de l'OCDE mais ils contiennent un principe exigeant des garanties appropriées pour des catégories spéciales de données (« données sensibles ») qui révèlent l'origine raciale, les opinions politiques ou religieuses, ou autres convictions relatives à la santé ou la vie sexuelle, ou qui concernent des condamnations pénales.¹⁵

Dispositions concernant les flux de données

Les principes de la Convention prévoient la libre circulation des données à caractère personnel entre les parties à la Convention qui offrent une protection équivalente¹⁶.

Dispositions concernant la poursuite de la coopération

Pour l'assistance mutuelle dans la mise en œuvre de la Convention, chaque partie à la Convention désigne une autorité chargée de fournir des informations sur son droit et sur sa pratique administrative en matière de protection des données¹⁷. En outre, les articles 18 à 20 établissent le *Comité consultatif* qui représente les États membres et fait des propositions concernant l'application de la Convention.

Dispositions concernant la mise en œuvre et l'exécution

Chaque État signataire s'engage à prendre, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données¹⁸, mais les modalités de cette mise en œuvre sont laissées à son appréciation. Aux termes de l'article 10, les États s'engagent à établir des « sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base ».

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données [STE n° 181]

Le 8 novembre 2001, un Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), concernant les autorités de contrôle et les flux transfrontières de données [STE n° 181] (COE, 2001) a été ouvert à la signature. Il a été signé par 21 États membres et ratifié par deux États.

Travaux en cours

Par le biais du Comité consultatif, le Conseil de l'Europe continue ses travaux dans le domaine de la protection de la vie privée et a adopté récemment un Guide relatif à l'élaboration de clauses contractuelles régissant la protection des données lors de communications de données à caractère personnel à des tiers non soumis à un niveau de protection des données adéquat, qui vise à étoffer et à affiner les clauses du contrat-type de 1992, de sorte que les deux documents peuvent être considérés comme complémentaires. Le *Groupe de projet sur la protection des données* du Conseil de l'Europe travaille également sur un projet de rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données à caractère personnel au moyen de la vidéosurveillance.

Table 6.1. **Tableau des instruments nationaux**

Pays	Ratification de la Convention 108	Législation cadre ayant trait à la protection de la vie privée et des données et visant :	
		Le secteur public	Le secteur privé
Australie		✓	
Autriche *	✓	✓	✓
Belgique *	✓	✓	✓
Canada		✓	Québec
République tchèque	✓	✓	✓
Danemark*	✓	✓	✓
Finlande*	✓	✓	✓
France*	✓	✓	✓
Allemagne*	✓	✓	✓
Grèce*	✓	✓	✓
Hongrie	✓	✓	✓
Islande	✓	✓	✓
Irlande*	✓	✓	✓
Italie*	✓		✓
Japon		✓	
Corée		✓	
Luxembourg*	✓	✓	✓
Mexique		✓	
Pays-Bas*	✓	✓	✓
Nouvelle-Zélande		✓	✓
Norvège	✓	✓	✓
Pologne	✓	✓	✓
Portugal*	✓	✓	✓
Espagne*	✓	✓	✓
Suède*	✓	✓	✓
Suisse	✓	✓	✓
Turquie			
Royaume-Uni*	✓	✓	✓
Etats-Unis		✓	

* Indique l'appartenance à l'Union européenne.

- c) Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel

Statut

Les *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel* du Haut Commissariat des Nations Unies aux droits de l'homme (Résolution 45/95 du 14 décembre 1990) (« Principes directeurs des Nations Unies ») (NU, 1990) ont été adoptés par l'Assemblée générale des Nations Unies conformément à l'article 10 de la Charte des Nations Unies. Cet article habilite l'Assemblée générale à faire des recommandations aux États membres. Les États membres doivent prendre en compte les principes directeurs lorsqu'ils introduisent des réglementations nationales relatives aux fichiers informatisés de données à caractère personnel, mais les procédures de mise en oeuvre de ces réglementations sont laissées à l'initiative de chaque État.

Portée

Les Principes directeurs des Nations Unies s'appliquent aux fichiers informatisés (publics ou privés) contenant des données à caractère personnel et peuvent être étendus (de manière facultative) aux fichiers manuels et aux fichiers concernant des personnes morales. La Partie A des Principes directeurs concerne les garanties minimales qui devraient être prévues dans les législations nationales. La Partie B des Principes directeurs concerne les données à caractère personnel détenues par les organisations internationales gouvernementales.

Principes de base

Les « Principes concernant les garanties minimales qui devraient être prévues dans les législations nationales » sont globalement similaires aux principes de base énoncés dans les Lignes directrices de l'OCDE. De plus, les Principes directeurs des Nations Unies restreignent la compilation des « données sensibles » dans le cadre du « Principe de non-discrimination »¹⁹.

Dispositions concernant les flux transfrontières de données

Le paragraphe 9 des Principes directeurs des Nations Unies recommande la libre circulation des flux transfrontières de données entre les pays présentant des « garanties comparables ».

Dispositions concernant la mise en œuvre et l'exécution

Concernant la législation nationale (Partie A), l'article 8 recommande que chaque pays établisse une autorité indépendante chargée de contrôler l'application des dispositions relatives à la vie privée dans les principes directeurs. En outre, en cas de violation des dispositions de la loi nationale mettant en œuvre ces principes, des « sanctions pénales ou autres devraient être prévues ainsi que des recours individuels appropriés ».

Concernant les organisations internationales gouvernementales (Partie B), la désignation d'une autorité de contrôle est aussi recommandée.

Travaux en cours

Un rapport de 1997 du Secrétaire général des Nations Unies (NU, 1997) examine la mise en œuvre des Principes directeurs au sein du système des Nations Unies et aux niveaux national et régional.

- d) Directive 95/46/CE de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Statut

La directive 95/46/CE du Parlement européen et du Conseil de l'Union européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« directive de l'Union européenne ») (UE, 1995) est un

instrument ayant force obligatoire que les 15 États membres de l'Union européenne devaient mettre en œuvre au plus tard le 24 octobre 1998.

Portée

Cette directive s'applique de manière générale au traitement de données à caractère personnel par un « responsable du traitement » établi dans un État membre de l'Union européenne²⁰. Elle s'applique aux données relatives aux personnes physiques, que ces données soient détenues par le secteur public ou le secteur privé. Elle couvre le traitement de données informatisé et la plupart des catégories de traitement manuel²¹.

Principes de base

Les principes de protection des informations contenus dans le Chapitre II de la directive de l'Union européenne sont plus larges et plus détaillés que ceux des Lignes directrices de l'OCDE. En plus des principes de l'OCDE, la directive de l'Union européenne contient, entre autres, des dispositions spéciales concernant les données sensibles²², des exigences d'information détaillées²³, des dispositions de notification²⁴, des droits d'opposition des personnes concernées pour se soustraire aux sollicitations commerciales²⁵, et de recours²⁶.

Dispositions concernant les flux transfrontières de données

La directive de l'Union vise à garantir les flux transfrontières de données à l'intérieur de l'Union européenne sur la base d'une protection équivalente assurée dans l'ensemble des États membres et elle autorise les transferts vers des pays tiers qui assurent une protection adéquate. Il n'est pas permis aux États membres de restreindre la libre circulation des données à caractère personnel entre États membres simplement pour des raisons de protection de la vie privée²⁷, en raison du niveau équivalent et élevé de protection assuré par la directive dans l'ensemble de la Communauté. Le transfert de données à l'extérieur de l'UE est possible à destination de pays tiers qui garantissent un degré de protection « adéquat »²⁸. Cette adéquation doit s'apprécier « au regard de toutes les circonstances relatives à un transfert ... en particulier, [en prenant] en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ». Il existe des exceptions, par exemple quand le consentement de la personne concernée a été obtenu²⁹.

Dispositions concernant la mise en œuvre et l'exécution

La directive de l'Union européenne définit le rôle de l'autorité de contrôle ou de l'organisme compétent en matière de protection des données dans un État membre, qui constitue un aspect essentiel de la mise en œuvre et de l'exécution de la législation nationale transposant la directive. Ces autorités doivent agir en toute indépendance et disposer d'un large éventail de pouvoirs, notamment de pouvoirs d'investigation et d'intervention et de la capacité d'ester en justice³⁰.

Concernant la mise en œuvre de ses dispositions, la directive de l'Union européenne prévoit des recours juridictionnels, des responsabilités et des sanctions³¹. Elle stipule que toute personne doit disposer d'un recours juridictionnel et a le droit d'obtenir du responsable du traitement une indemnisation du préjudice subi du fait d'un traitement illicite. Le choix des sanctions administratives, civiles ou pénales à adopter doit être fait par chaque État membre.

Dispositions concernant la poursuite de la coopération

L'article 28 prévoit que les autorités de contrôle doivent coopérer entre elles selon les besoins, notamment en échangeant toute information utile.

La directive établit deux organes, l'un consultatif (article 29) et l'autre décisionnel (article 31), afin d'assister la Commission européenne pour les questions relatives au traitement des données.

Travaux en cours

Le Groupe institué par l'article 29 a déjà publié un certain nombre de rapports et de recommandations, notamment « Premières orientations relatives aux transferts de données personnelles vers des pays tiers - Méthodes possibles d'évaluation du caractère adéquat de la protection » (UE, 1997a) et « Évaluation des codes d'autoréglementation sectoriels » (UE, 1998).

Autres initiatives

Le 15 décembre 1997, la directive 97/66/CE (UE, 1997b) a été adoptée par le Parlement européen et le Conseil. Cette directive complète la directive 95/46/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Elle prévoit l'harmonisation des dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des télécommunications, ainsi que la libre circulation de ces données et des équipements et services de télécommunications dans la Communauté.

e) Accord général sur le commerce des services

L'*Accord général sur le commerce des services* (AGCS) est un accord multilatéral qui vise à promouvoir un libre échange des services. L'AGCS est administré par l'*Organisation mondiale du commerce* (OMC)³². L'article XIV indique que l'AGCS n'interdit pas aux États membres d'adopter les mesures nécessaires « à la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination de données personnelles, ainsi qu'à la protection du caractère confidentiel des dossiers et comptes personnels »³³. Toutefois, l'article XIV limite ce que peut faire un pays en matière de protection de la vie privée en lui imposant de veiller à ce qu'aucune mesure de cette nature ne soit appliquée de façon discriminatoire et ne constitue un obstacle déguisé aux échanges de services.

2. Colloques internationaux et forums de discussion sur la protection de la vie privée

Les colloques internationaux et forums de discussion jouent un rôle important en contribuant à l'échange d'informations, à l'éducation et à l'élaboration d'instruments en matière de protection de la vie privée.

a) Conférences internationales annuelles des commissaires à la protection des données

Depuis 1979, une Conférence internationale des commissaires à la protection des données a lieu chaque année. Ces Conférences n'ont pas de statut légal particulier et ne votent pas de résolutions. Elles constituent plutôt un lieu d'échange d'informations. La 20^{ème} Conférence des autorités de protection des données s'est tenue à Saint-Jacques-de-Compostelle (Espagne)³⁴.

b) Conférences des commissaires européens à la protection des données

Les conférences annuelles des commissaires à la protection des données de l'Union européenne offrent l'occasion de développer des approches communes à l'égard de la protection de la vie privée et d'aborder des questions d'actualité comme les télécommunications et les fichiers de police.

c) Groupe de travail international sur la protection des données dans les télécommunications

Le *Groupe de travail international sur la protection des données dans les télécommunications*, sous la conduite du Commissaire à la protection des données de Berlin, a été créé par les commissaires à la protection des données d'un certain nombre de pays en vue d'améliorer la protection de la vie privée et des données dans les télécommunications et les médias. Le « Mémoire de Budapest-Berlin » concernant la protection des données sur l'Internet examine les questions entourant la protection juridique et technique de la vie privée des utilisateurs de l'Internet (*International Working Group on Data Protection in Telecommunications*, 1996)³⁵.

d) Organisation internationale de normalisation (ISO)

L'Organisation internationale de normalisation (ISO)³⁶ est une fédération mondiale réunissant les organismes de normalisation nationaux d'environ 130 pays. Les travaux de l'ISO aboutissent à des accords internationaux publiés sous la forme de Normes internationales. En mai 1996, le *Comité de l'ISO pour la politique en matière de consommation* a adopté une résolution unanime en faveur d'un projet visant à élaborer une norme internationale sur la protection de la vie privée basée sur le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation. Un *Groupe consultatif ad hoc sur la confidentialité* a entrepris une étude pour le compte de l'ISO pour voir s'il était nécessaire, eu égard aux progrès technologiques des structures mondiales de l'information, d'établir une norme internationale pour traiter la question de la confidentialité des informations, mesurer la protection de la vie privée et assurer une harmonisation mondiale.³⁷ Le Groupe consultatif a conclu en juin 1999 qu'il était prématuré de se prononcer sur l'opportunité et l'intérêt pratique de l'élaboration par l'ISO de normes internationales intéressant la protection de la vie privée.

e) Chambre de commerce internationale

La Chambre de commerce internationale (CCI)³⁸, qui représente les entreprises internationales dans le monde entier, a produit un certain nombre de documents et de codes sectoriels sur la protection de la vie privée et les flux d'informations, notamment tout un éventail de codes et principes en matière de marketing, et en particulier des principes directeurs à l'égard de la publicité sur Internet, qui contient des dispositions pour la protection de la vie privée³⁹. La CCI a également publié un projet de contrat type pour les flux transfrontières de données à caractère personnel qui s'appuie sur le contrat type CCI/Conseil de l'Europe/Commission européenne de 1992.

f) Fédération Internationale des associations de vente par correspondance

La *Fédération Internationale des associations de vente par correspondance* (IFDMA) est une structure de collaboration des associations de la vente directe nationales et régionales. Un de ses objectifs est de promouvoir les programmes d'éducation des consommateurs et d'autorégulation menés par l'industrie. Les « principes en ligne » pour la protection des données formulés par l'IFDMA encouragent les entreprises pratiquant la vente directe à afficher en ligne leur politique en matière de protection de la vie privée d'une manière facile à trouver, à lire et à comprendre. Ces principes comprennent des dispositions spéciales concernant les activités des enfants en ligne.

g) Electronic Commerce Europe

Electronic Commerce Europe (EDE) est un groupe d'entreprises et d'associations européennes du commerce électronique qui travaillent à la formulation d'un *Code de conduite pour le commerce électronique*.

h) Initiatives en ligne pour l'échange d'informations sur la protection de la vie privée

Un certain nombre d'organisations non gouvernementales s'intéressant à la protection de la vie privée ont créé des sites Web pour fournir des informations sur les questions relatives à la protection de la vie privée dans les communications en ligne. On peut mentionner, entre autres :

- L'*Electronic Privacy Information Center*⁴⁰ (EPIC), centre de recherche pour la défense des intérêts du public créé pour attirer l'attention du public sur les nouvelles questions que l'environnement en ligne soulève pour les libertés publiques et pour protéger la vie privée.
- Le *Center For Democracy and Technology*⁴¹ (CDT) organisation de défense des intérêts du public qui agit en faveur des libertés publiques et des valeurs démocratiques dans les nouvelles technologies de l'informatique et des communications.
- *Privacy International*⁴², qui est un groupe de défense des droits de l'homme exerçant sa vigilance contre la surveillance des personnes par les gouvernements et les entreprises.
- *PrivacyExchange.Org*⁴³, créé pour fournir des informations actualisées sur les législations et pratiques nationales en matière de protection des données et pour distribuer des modèles de politiques, d'accords et de codes de conduite.

B. Instruments nationaux

ALLEMAGNE

Législation

Lois fédérales horizontales

La *Loi fédérale de protection des données* (1990)⁴⁴ allemande s'applique aux fichiers informatisés ou manuels concernant les personnes physiques. Cette loi fait une distinction entre les responsables de fichier dans le secteur public et dans le secteur privé. Les fichiers nominatifs du secteur public doivent être enregistrés auprès du *Commissaire fédéral à la protection des données*, autorité indépendante désignée par le Parlement. Les autorités de contrôle pour le secteur privé sont désignées conformément aux lois de chaque État (*Land*) allemand. Les organisations privées sont tenues, dans certains cas, de nommer des contrôleurs de la protection des données pour veiller à l'observation de la loi.

Toute personne peut déposer une plainte auprès du Commissaire fédéral à la protection des données si elle pense qu'une autorité fédérale a porté atteinte à ses droits en collectant, traitant ou utilisant des données la concernant⁴⁵. De même, les plaintes contre les organisations du secteur privé peuvent être déposées devant les autorités de contrôle des Länder. Concernant les sanctions, la loi instaure des sanctions administratives et des délits pénaux⁴⁶.

Autres lois fédérales comportant des dispositions de protection de la vie privée

Le gouvernement fédéral allemand a promulgué un nombre appréciable de lois et règlements⁴⁷ sur des questions spécifiques relatives à la protection de la vie privée, concernant notamment : les archives et registres nationaux ; les statistiques fédérales ; les registres de la population ; la conservation et le transfert de données à caractère personnel concernant les étrangers en Allemagne (*Loi sur le registre central des étrangers* (1994)) ; et les télécommunications (*Loi fédérale sur les télécommunications* (1996) et *Décret sur la protection des données des exploitants de télécommunications*).

L'article 2 de la *Loi fédérale sur les services d'information et de communication* (1997)⁴⁸ régit le traitement des données à caractère personnel dans l'environnement des réseaux. Cette loi mentionne l'utilisation anonyme des téléservices, les dispositifs techniques réduisant au minimum la quantité de données à caractère personnel collectées et les procédures pour obtenir un consentement électronique. La *loi relative à la protection des données dans le cadre des téléservices* (2001)⁴⁹ régit expressément le traitement des données à caractère personnel des usagers par les prestataires de services d'information. La loi prévoit l'anonymat dans l'utilisation des téléservices, limite au minimum la quantité de renseignements à caractère personnel recueillis par les prestataires et prévoit la possibilité, pour les usagers, de consentir par voie électronique à un traitement plus poussé des données qui les concernent, ainsi que les procédures nécessaires.

Lois des Länder (États)

Chaque *Land* a sa propre loi de protection des données applicable à son secteur public, ainsi que sa propre autorité de protection des données⁵⁰. Les Commissaires à la protection des données de la Fédération et des Länder tiennent régulièrement des conférences⁵¹. Les Länder ont également énoncé, dans leur *Traité sur les services de médias*, des règles relatives à certains services d'information qui correspondent aux règles formulées dans la *loi fédérale relative à la protection des données dans le cadre des téléservices*.

Mise en œuvre de la directive de l'Union européenne

Le gouvernement fédéral et les Länder travaillent actuellement à une nouvelle législation destinée à mettre en œuvre la directive de l'Union européenne⁵². Certains Commissaires des Länder ont proposé des projets de transposition et ont publié des lignes directrices sur les flux transfrontières de données vers les pays n'ayant pas de dispositions de protection adéquates.

Instruments d'autorégulation

L'approche à l'égard de la protection de la vie privée en Allemagne repose actuellement davantage sur les lois que sur les mécanismes d'autorégulation.

AUSTRALIE

Législation

Législation du Commonwealth d'Australie (législation fédérale)

La *Privacy Act* de 1988 (loi fédérale) est le principal texte régissant la protection de l'information à caractère personnel dans le secteur public fédéral et dans le secteur privé.⁵³ Cette loi énonce 11 principes de protection de la confidentialité de l'information pour le secteur public fédéral et 10 principes de protection de la vie privée à l'échelle nationale pour les organisations du secteur privé, qui sont basés sur les lignes directrices de l'OCDE. Ces principes de protection de la confidentialité/vie privée couvrent toutes les étapes du traitement de l'information à caractère personnel et fixent des normes pour la collecte, l'utilisation, la divulgation, la qualité et la sécurité de cette information. Ils instituent également l'obligation de permettre aux citoyens d'avoir accès à l'information qui les concerne et de la corriger le cas échéant.

La *Privacy Act* établit également la fonction de *Federal Privacy Commissioner* (Commissaire fédéral à la protection de la vie privée) qui peut recevoir des plaintes, conduire des enquêtes et prononcer des décisions (y compris des ordres d'indemnisation) qui peuvent être rendus exécutoires par la *Federal Court of Australia*.⁵⁴

Autres textes législatifs fédéraux comportant des dispositions relatives à la vie privée

D'autres lois du Commonwealth australien protègent la confidentialité de certains types d'information, comme les condamnations pénales passées que l'on n'a plus le droit de mentionner (*Le Crimes Act 1914*, Partie VIIC, protège les personnes contre l'utilisation non autorisée des informations sur certaines condamnations pénales après dix ans) et les informations fiscales (*Taxation Administration Act 1953*), ainsi que pour certaines procédures comme l'interception des télécommunications et la divulgation d'informations personnelles par les compagnies de télécommunications (*Telecommunications Act 1997*). La *Data-matching Program (Assistance and Tax) Act 1990* prévoit des mesures de protection de la vie privée en liaison avec le rapprochement d'informations de caractère personnel concernant le fisc et les prestations de sécurité sociale par des Ministères gouvernementaux du Commonwealth.

Lois des États et Territoires

Plusieurs États et territoires ont légiféré pour mettre en place des dispositions de protection de la vie privée, soit à l'égard du secteur public, soit en ce qui concerne l'information médicale à caractère personnel. D'autres États ont mis en place des régimes de protection de la vie privée par voie administrative qui traduisent les principes énoncés dans la *Privacy Act* fédérale.⁵⁵

Instruments d'autorégulation

La *Privacy Act* fédérale prévoit également l'élaboration de codes de protection de la vie privée à l'intention des entreprises et industries du secteur privé qui peuvent être approuvés par le Commissaire à la protection de la vie privée. Une fois approuvé un code de protection de la vie privée, celui-ci remplace les normes législatives bien que les codes doivent au minimum correspondre à ces normes.⁵⁶

AUTRICHE

Législation

Lois fédérales horizontales

La *Loi fédérale sur la protection des données de 1978 (Datenschutzgesetz, BGBl. Nr.565/1978)* régit l'utilisation des données informatisées dans le secteur public et le secteur privé, crée un système central d'enregistrement et prévoit des recours civils et des sanctions pénales⁵⁷. Une nouvelle loi est en préparation pour transposer la directive européenne sur la protection des données.

Une Commission indépendante (la *Datenschutzkommission*) est chargée d'appliquer la loi, d'administrer le système d'enregistrement et d'autoriser les flux transfrontières de données. La Commission agit en réponse à des plaintes particulières contre des maîtres de fichiers publics, et elle peut prendre des sanctions contre certains agissements comme les violations des autorisations de flux transfrontières de données. Il existe aussi un *Conseil pour la protection des données* auquel la Commission peut se remettre pour obtenir un avis sur certaines questions. Les plaintes contre les maîtres de fichiers privés doivent être déposées devant les tribunaux.

La Chambre de Commerce et la Chancellerie fédérale assurent le fonctionnement d'un tribunal arbitral, le *Schlichtungsstelle-Datenschutz*, qui examine les plaintes contre les entreprises qui n'ont pas satisfait à la demande d'une personne de consulter, corriger ou supprimer des informations à caractère personnel la concernant.

Autres lois fédérales comportant des dispositions de protection de la vie privée

De nombreuses lois fédérales autrichiennes comportent des aspects relatifs à la protection de la vie privée. Par exemple, la *Loi autrichienne sur les télécommunications (1997)*⁵⁸ impose des obligations de confidentialité et de protection des données aux fournisseurs de services de télécommunications publiques. L'utilisation d'informations à caractère personnel par les entreprises de vente directe est régie par la Section 268 du *Code des entreprises (1994)*⁵⁹. Enfin, la *Loi sur le génie génétique de 1994* contient des dispositions protégeant les données dans ce domaine.

Mise en œuvre de la directive de l'Union européenne

Un premier projet de texte pour le *Datenschutzgesetz* a été soumis récemment au Parlement⁶⁰.

Lois des Länder (États)

On examine actuellement, dans le contexte de la mise en œuvre de la directive de l'Union européenne, le rôle que jouera chaque *Land* dans la protection des données.

Instruments d'autorégulation

Il n'existe pas de code de conduite en Autriche traitant exclusivement de la protection de la vie privée mais les entreprises du secteur bancaire ont mis en place des codes contenant des clauses générales relatives à cette question.

BELGIQUE

Constitution

La *Constitution belge* énonce les droits relatifs à la protection de la vie privée dans ses articles 22 et 32.

Législation

Lois horizontales

En Belgique, la *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (1992) s'applique aussi bien au secteur public qu'au secteur privé. Cette loi est complétée par des Arrêtés royaux concernant, par exemple, les données sensibles et les informations relatives aux condamnations pénales. La *Commission consultative de la protection de la vie privée*, organe indépendant au sein du *ministère de la Justice* surveille l'application de la loi⁶¹. La Commission tient un registre des traitements des données et peut aussi conseiller le gouvernement en matière de protection de la vie privée.

Concernant les moyens de recours, les personnes concernées peuvent s'adresser au *Tribunal de première instance* pour faire valoir leurs droits aux termes de la loi. Cette loi établit aussi des sanctions pénales pour les violations des obligations de protection de la vie privée⁶².

Autres lois comportant des dispositions de protection de la vie privée

La *Loi du 30 juin 1994* traite de la protection de la vie privée dans le contexte de l'interception et de l'enregistrement des télécommunications privées.

Mise en œuvre de la directive de l'Union européenne

Un projet de loi destiné à transposer la directive et basé sur la structure de la loi de 1992 est actuellement soumis au Parlement belge⁶³.

Instruments d'autorégulation

L'Association des fournisseurs de service Internet de Belgique a un Code de conduite adopté par l'Assemblée plénière qui demande à ses membres de se conformer à la législation de la protection de la vie privée dans l'utilisation des données à caractère personnel de leurs clients⁶⁴.

CANADA

Législation

Lois fédérales

La *Loi sur la protection des renseignements personnels* (1983)⁶⁵ s'applique à la quasi-totalité des institutions du secteur public fédéral canadien. Cette loi régit la confidentialité, la collecte, la correction, la divulgation, la conservation et l'utilisation des informations à caractère personnel, et elle confère aux personnes concernées le droit d'examiner les informations détenues à leur sujet et de demander la correction des erreurs. Cette loi repose sur les principes des Lignes directrices de l'OCDE.

Le *Commissaire à la protection de la vie privée*, nommé par le Parlement, enquête sur les plaintes et contrôle l'application des dispositions de la loi par les institutions fédérales. Le Commissaire est habilité à conduire des enquêtes, à essayer de résoudre les litiges et à émettre des recommandations. Les litiges concernant le droit d'accès aux informations à caractère personnel qui ne se résolvent pas de cette manière peuvent être portés devant le *Tribunal fédéral* pour un recours en révision.

L'approche fédérale à l'égard de la protection de la vie privée dans le secteur privé

Le Gouvernement fédéral canadien a introduit le 1er octobre 1998 une législation relative à la vie privée destinée à protéger les informations à caractère personnel dans le secteur privé. Le projet de loi C-54 *sur la protection des informations à caractère personnel et les documents électroniques*, a fait l'objet d'une deuxième lecture et est actuellement étudié par le Comité permanent de l'industrie, qui fera rapport au Parlement au printemps de 1999. Cette législation étendra d'abord la protection de la vie privée au secteur privé sous tutelle fédérale, ainsi qu'aux échanges interprovinciaux et internationaux d'informations à caractère personnel. Trois ans plus tard, la législation s'appliquera aux autres organisations privées qui relèvent des juridictions provinciales. Si une province promulgue une législation sensiblement de même nature, les organisations commerciales qui opèrent sous sa juridiction seront soumises à cette législation provinciale. A l'heure actuelle, seule la province de Québec s'est dotée d'une telle législation. Les droits et obligations énoncés dans le projet de loi sont ceux de la version préliminaire du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, qui est une norme nationale reconnue de protection de la vie privée, calquée sur le modèle des Lignes directrices de l'OCDE. Les particuliers bénéficient de droits d'accès et de rectification et le Commissaire à la protection de la vie privée supervisera les enquêtes et l'établissement de rapports sur les plaintes. Le Commissaire dispose des pouvoirs d'un médiateur mais les plaignants peuvent porter les questions non résolues devant le *Tribunal fédéral*, comme peut le faire aussi le Commissaire, et le Tribunal a le pouvoir de prendre des décisions contraignantes et d'allouer des dommages et intérêts.

Lois des Provinces

La plupart des Provinces ont adopté une législation de protection de la vie privée gouvernant le secteur public et, dans la majorité des cas, cette législation repose sur les principes contenus dans les Lignes directrices de l'OCDE⁶⁶. Diverses lois sectorielles garantissent la protection de la vie privée dans des domaines comme les informations de santé des personnes⁶⁷.

Le Québec est la seule province où une législation générale, la loi sur la protection des renseignements personnels dans le secteur privé (1993), régit le traitement des informations à caractère personnel par les organisations du secteur privé, dont les entreprises, les entreprises unipersonnelles, les partenariats, les organisations et les associations. La loi régit notamment la collecte et l'utilisation des informations de caractère personnel et elle donne aux particuliers des droits d'accès et de rectification ; les litiges sont portés devant la Commission d'accès à l'information, qui est l'organisme chargé de superviser et faire appliquer les droits d'accès à l'information et au respect de la vie privée dans le secteur public au niveau de la province. Il faut noter que cette loi comporte des dispositions spécifiques visant les listes de noms utilisées à des fins de marketing et les transferts d'informations sur des résidents du Québec à des tiers extérieurs à la province.

Instruments d'autorégulation

Le Code type de l'Association canadienne de normalisation

Il existe au Canada un code type concernant la protection de la vie privée, qui recueille une large adhésion. Le *Code type sur la protection des renseignements personnels* a été élaboré par le *Comité technique sur la protection de la vie privée*⁶⁸ de l'Association canadienne de normalisation (CSA) et a été adopté comme Norme nationale par le *Conseil canadien des normes* en 1996⁶⁹. Ce Code s'inspire des Lignes directrices de l'OCDE, mais il demande aussi aux entreprises de désigner une personne qui devra s'assurer du respect des principes énoncés et à qui les plaintes pourront être adressées.

La CSA a produit un manuel intitulé *Making the CSA Privacy Code Work for You*⁷⁰, pour apporter une aide à l'élaboration de codes conformes (qui peuvent être certifiés par le *Quality Management Institute*, qui est une division de la CSA). Pour assurer le respect permanent d'un code, le manuel souligne l'importance des audits indépendants réalisés par des contrôleurs dûment certifiés. Les codes du secteur privés peuvent recevoir une certification de conformité à la norme de la CSA délivrée par un contrôleur qualité et une entreprise peut citer la norme dans un enregistrement ISO9000. Il existe de multiples façons pour une entreprise de démontrer sa conformité à la norme ; ainsi le *Modèle de code* de l'Association des banquiers canadiens a été vérifié par Price Waterhouse.

Autres initiatives

Un certain nombre d'entreprises et d'associations ont développé ou sont en train d'élaborer des codes de protection de la vie privée basés sur celui de la CSA, notamment Stentor (l'alliance des prestataires de télécommunications), l'Association canadienne de marketing, l'Association des banquiers canadiens, le Bureau d'assurance du Canada, le Conseil canadien des normes de radiotélévision et l'Association médicale canadienne (AMC).

Instruments concernant la protection de la vie privée dans les communications en ligne

Le *Code de conduite*⁷¹ volontaire de l'Association canadienne des fournisseurs Internet (ACFI) demande aux membres de l'ACFI de respecter et de protéger la vie privée de leurs utilisateurs et de se conformer à toutes les lois applicables. Chaque membre doit établir un processus pour recevoir et traiter les plaintes.

CORÉE

Constitution

La Constitution coréenne stipule que tout citoyen a droit au respect de sa vie privée (article 17) et à la liberté de communication (article 18).

Législation

Lois gouvernant le secteur public

La *loi sur la protection des informations personnelles par les organisations publiques* régit la protection des informations à caractère personnel dans le secteur public. Cette loi repose sur les principes des Lignes directrices de l'OCDE et elle oblige les organisations publiques à agir avec précaution et à promouvoir la confidentialité dans le traitement des données à caractère personnel. Les citoyens ont le droit d'accéder aux données personnelles les concernant et ils ont la possibilité de les faire corriger.

Autres lois comportant des dispositions de protection de la vie privée

La *loi sur la protection des informations en matière de crédit* porte sur la protection des données à caractère personnel dans les transactions financières. Par exemple, la loi interdit à une institution financière de révéler ou de partager des données personnelles et financières sans le consentement écrit de la personne concernée. La Corée a aussi une loi sur la *Protection de la confidentialité dans les communications*.

Approche à l'égard de la protection de la vie privée dans le secteur privé

La *loi sur le développement de l'utilisation des réseaux de communications* a été amendée en janvier 1999 afin d'institutionnaliser la protection des données à caractère personnel dans le secteur privé, conformément aux principes énoncés dans les Lignes directrices de l'OCDE. La loi révisée, qui entrera en vigueur en janvier 2000, autorise le gouvernement à imposer des restrictions spécifiées aux fournisseurs de services d'information et de télécommunications lorsque ceux-ci font une utilisation abusive ou détournée de données à caractère personnel.

Instruments d'autorégulation

A l'heure actuelle, il n'existe pas d'initiatives d'autorégulation dans le secteur privé en Corée, mais des discussions devraient également avoir lieu à ce sujet.

DANEMARK

Constitution

Aux termes de la section 72 de la Constitution qui énonce le caractère sacré du foyer, il est interdit, en l'absence d'autorisation préalable d'un tribunal, de fouiller le logement d'une personne, d'ouvrir son courrier ou d'intercepter ses communications téléphoniques. Il est généralement admis dans la théorie juridique danoise que cette section peut s'interpréter comme couvrant aussi les données stockées sous forme électronique et toutes les formes de télécommunications. Les autorités ne peuvent, par exemple, ouvrir et examiner du courrier électronique sans autorisation préalable. Elles ne peuvent intercepter le message et le consulter sur les réseaux de télécommunications que si elles en ont obtenu l'autorisation d'un tribunal. La principale règle étant qu'une fouille nécessite l'autorisation préalable d'un tribunal, une fouille sans autorisation préalable ne peut avoir lieu que dans des circonstances exceptionnelles où elle apparaît absolument nécessaire. Une autorisation générale à cet effet est accordée conformément aux dispositions de la loi sur les procédures civiles et criminelles. En dehors du champ des procédures civiles, une telle autorisation est donnée dans de nombreux textes de lois permettant des recherches administratives, par exemple les enquêtes de l'Autorité chargée de la surveillance des données, pour localiser les systèmes de fichiers publics.

Législation

La loi sur l'accès du public (§4, sect.1) garantit à tout citoyen l'accès aux documents faisant partie de décisions des autorités publiques. L'accès général aux documents est toutefois limité par la section 3 du § 4, car la personne qui demande accès doit pouvoir indiquer la raison pour laquelle elle demande l'accès.

Les documents suivants ne sont pas accessibles : dossiers de poursuites pénales, demandes et procédures concernant l'emploi de fonctionnaires et documents à usage purement interne. Ces exclusions peuvent être subdivisées en deux catégories : i) les données à caractère personnel qui concernent les personnes physiques au sens du § 12 et ii) les catégories de données auxquelles l'accès est refusé pour des questions d'ordre public, conformément au § 13. Un exemple de données de la première catégorie pourrait être l'affiliation politique d'une personne. Un exemple de considération de politique publique empêchant de donner l'accès aux données de la deuxième catégorie pourrait être la protection de la sécurité nationale.

Les lois danoises sur les fichiers publics et privés sont en vigueur depuis 1979. Celles-ci prévoient la protection de la vie privée vis-à-vis aussi bien des organismes gouvernementaux que des systèmes de fichiers détenus par des entités privées.

La loi relative aux systèmes de fichiers publics s'applique aux systèmes de fichiers informatisés constitués par les autorités publiques, qui contiennent des données à caractère personnel, au sens de la section 1 du § 1. La loi ne s'applique qu'au secteur public.

L'une des finalités de la loi sur les systèmes de fichiers privés est de faire en sorte que les données à caractère économique et personnel sur des citoyens, des institutions, des sociétés et des entreprises ne soient enregistrées par des personnes privées que dans la mesure où elles visent des intérêts légitimes et que les données consignées fassent l'objet d'un traitement satisfaisant. La loi énonce à l'égard des personnes privées une interdiction générale de traitement systématique de données de caractère personnel, mais elle prévoit cependant quelques exceptions. La loi vise tout *traitement systématique* (recueil, enregistrement et communication) de *données de caractère économique ou personnel*, effectué par des personnes privées (individus ou entreprises) par des *moyens électroniques* ou, dans certains cas par traitement *manuel*.

La loi danoise sur les médias définit les responsabilités des organes d'information de masse (que ceux-ci utilisent les supports d'informations traditionnels ou les nouvelles technologies de l'information). La loi sur les médias est étroitement liée au Code pénal, dans la mesure où plusieurs cas d'infractions dans le secteur des médias, sanctionnées par cette loi, se réfèrent aux règles régissant la vie privée dans le Code pénal.

Le Code pénal (§152) interdit aux agents du secteur public le traitement ou l'utilisation illicite d'informations confidentielles obtenues dans le cadre de leurs attributions. Cette section jette également les bases juridiques nécessaires pour condamner à des peines d'amende les fonctionnaires qui ne respectent leur devoir de confidentialité. Cet article stipule que le simple fait d'obtenir des informations est autorisé, mais qu'il est illégal de traiter des informations de caractère personnel ou d'en faire une utilisation abusive. Cependant, l'obtention des informations peut faire l'objet de sanctions disciplinaires traditionnelles. Le paragraphe §152a-d précise que le devoir de confidentialité (et les sanctions qui s'y rattachent) s'étend également aux personnes n'ayant pas la qualité d'agent de l'État mais qui, d'une façon ou d'une autre, sont chargées de mission de service public.

Le premier alinéa du paragraphe §263 du Code pénal vise les cas d'ouverture du courrier d'autrui, de fouille de locaux privés ou d'écoute de conversations. Ces règles peuvent facilement s'interpréter comme s'appliquant au cas dans lequel une personne accède illégalement au courrier électronique d'une autre personne ou intercepte des messages via les réseaux de télécommunications. L'alinéa 2 couvre le cas d'une personne qui accède illégalement à des programmes ou des informations à caractère personnel destinés à être utilisés sur un système informatique. Cet alinéa s'applique également à l'interception des transmissions de données.

Aux termes du paragraphe §264d, il est illégal de transmettre des informations ou des images concernant la vie privée d'autres personnes. Avec les nouvelles possibilités offertes par les réseaux, la diffusion de ce type d'informations peut désormais concerner un éventail beaucoup plus grand de personnes qu'autrefois.

L'Autorité chargée de la surveillance des données supervise des systèmes d'archivage aussi bien publics que privés. Elle relève du Ministère de la Justice, mais le Ministère ne peut être saisi de plaintes la concernant et il n'est pas habilité à donner des ordres à l'Autorité ; en d'autres termes, celle-ci est indépendante. Cette indépendance fonctionnelle constitue un élément important garantissant l'intégrité de la personne concernée.

Mise en œuvre de la directive de l'Union européenne

Une proposition de transposition de la directive de l'Union européenne a été présentée au Parlement danois (le *Folketinget*) le 30 avril 1998.

Instrument d'autorégulation

L'Ombudsman pour les questions intéressant les consommateurs élabore actuellement un ensemble de règles déontologiques destinées à être mises en œuvre sur Internet, mais on ne dispose actuellement d'aucune information quant à la date à laquelle ces travaux seront achevés.

Sont également à l'origine d'autres initiatives réglementaires :

- Le Fabel, qui est un organisme chargé de promouvoir une utilisation responsable du courrier électronique.

- Le FIB, qui est un organisme pour les utilisateurs d'Internet et qui s'attache à défendre les droits de ces utilisateurs.
- Le FIL, qui est une organisation de fournisseurs de service Internet. Cette organisation a travaillé à l'élaboration d'un ensemble de règles visant à protéger les utilisateurs.

ESPAGNE

Constitution

L'article 18.4 de la *Constitution espagnole* stipule que « la loi limitera l'utilisation du traitement de données afin de garantir le respect de la vie privée personnelle et familiale des citoyens et le plein exercice de leurs droits ».

Législation

Lois horizontales

La *Loi de régulation du traitement automatisé des données à caractère personnel* (1992)⁷² s'applique aux fichiers informatisés dans le secteur public et le secteur privé. Une autorité publique indépendante, l'*Agence de protection des données*⁷³ surveille sa mise en œuvre. L'Agence délivre des autorisations préalables pour la création de bases de données, reçoit les plaintes et peut émettre des ordres concernant les infractions à la loi dans le secteur public. Elle a récemment publié des « Recommandations pour les utilisateurs de l'Internet » qui avertissent les utilisateurs des risques concernant la protection de la vie privée liés à l'utilisation de l'Internet.

La loi stipule que les peines infligées seront proportionnées à la nature et à l'ampleur de l'infraction⁷⁴.

Autres lois comportant des dispositions de protection de la vie privée

Il existe en Espagne une loi sur les statistiques publiques⁷⁵ comportant des dispositions de protection de la vie privée.

Mise en œuvre de la directive de l'Union européenne

Des travaux de révision de la législation sur la protection de la vie privée sont en cours en vue de la rendre conforme à la directive de l'Union européenne.

Instruments d'autorégulation

L'*Association espagnole du commerce électronique* (qui fait partie de l'*Association espagnole du marketing direct*) a un code de conduite concernant la protection de la vie privée sur l'Internet⁷⁶. Ce Code avertit ses membres des implications que les activités conduites sur l'Internet ont en matière de protection de la vie privée, en spécifiant qu'il faut informer les utilisateurs de leurs droits d'accès, de rectification et de suppression.

ÉTATS-UNIS

Constitution

La Constitution des États-Unis ne mentionne pas explicitement un droit au respect de la vie privée. Toutefois, la jurisprudence a reconnu que la Constitution confère un tel droit restreignant certaines activités ou violations par les pouvoirs publics de la vie privée, au sens physique du terme.

Législation

Lois sectorielles fédérales

Les États-Unis ne possèdent pas de législation horizontale fédérale ou de normes de base de protection de la vie privée d'application obligatoire. Ce pays a plutôt recours à un assemblage d'autorégulation, de législation sectorielle, d'activités de sensibilisation et d'autorité d'application. Par exemple, la *Federal Trade Commission* (FTC) use de son pouvoir pour empêcher les pratiques commerciales déloyales et/ou de nature à induire en erreur, et d'autres agences fédérales appliquent des dispositions relatives à la protection de la vie privée visant les secteurs qu'elles réglementent, tels que la santé, les transports et les services financiers.

Le Congrès a adopté une législation pour protéger certains renseignements personnels particulièrement sensibles tels que l'information concernant les enfants, et les dossiers financiers et médicaux. On trouvera ci-après quelques-uns des textes les plus récents :

- **Information concernant les enfants.** La *Childrens's Online Privacy Protection Act* (Loi sur la protection de la vie privée des enfants en ligne) de 1998 exige que les sites s'adressant aux enfants de moins de 13 ans obtiennent le consentement parental vérifiable avant de recueillir des informations personnelles auprès des enfants et de les utiliser. La FTC a publié en avril 2000 des règles d'application de cette loi qui obligent les sites à obtenir l'accord parental par courrier, télécopie, carte de crédit ou signature numérique avant de divulguer à un tiers un renseignement à caractère personnel concernant un enfant.
- **Information financière.** La *Financial Services Modernization Act* (Loi de modernisation des services financiers) de 1999 (Loi Gramm-Leach-Bliley) oblige les banques et les autres institutions financières qui s'échangent ou vendent de l'information confidentielle relative à leurs clients à suivre des politiques clairement définies de protection de la vie privée et à reconnaître aux consommateurs le droit de s'exclure du partage d'information avec des tiers.
- **Dossiers médicaux.** Le *Department of Health and Human Services* (ministère de la Santé) a publié de nouvelles règles de protection de la vie privée dans le contexte médical en application de la *Health Insurance Portability and Accountability Act* de 1996. Ces règles comprennent des normes de protection de la confidentialité des renseignements médicaux nominatifs qui sont communiqués par voie électronique, sur papier ou oralement. En juillet 2001, le ministère de la Santé a publié ses premiers éléments d'orientation pour clarifier certaines dispositions du règlement, notamment la question de savoir si les membres de la famille d'un patient peuvent faire remplir une ordonnance pour ce dernier.

Indépendamment de ces textes, le Congrès avait auparavant adopté une législation sectorielle concernant : la confidentialité financière [*Right to Financial Privacy Act* (1978) ; *Fair Credit Reporting Act* (1970, amendée en 1996)] ; la confidentialité des communications [*Telephone Consumer Protection Act* (1934, amendée en 1991 et enfin en 1994) ; *Telecommunications Act* de 1996 ; *Electronic*

Communications Privacy Act (1986)] ; ainsi que d'autres dispositions diverses relatives à la protection de la vie privée [*Driver's Privacy Protection Act* de 1994 (amendée en 1996), *Video Privacy Protection Act* de 1998 ; *Cable Communications Privacy Act* de 1984 (amendée pour la dernière fois en 1992) ; *Privacy Protection Act* de 1980 ; *Family Education Rights and Privacy Act* (1974, amendée en 2000)].

L'utilisation d'informations personnelles détenues par les agences du gouvernement fédéral est réglementée par la *Privacy Act* (1974)⁷⁷ qui énonce les *Principes d'information équitable* aux fins de traitement des données personnelles. L'*Office of Management and Budget* est chargé de surveiller l'application de cette loi, qui confère aux personnes concernées un droit d'action pouvant aboutir à des dommages-intérêts et/ou à une injonction. La loi prévoit également des sanctions pénales en cas d'infraction délibérée à la loi.

Lois des États

Dans un certain nombre d'États, la Constitution garantit un droit à la vie privée. Les États suivent généralement le modèle sectoriel fédéral et établissent des lois renforçant la protection de la vie privée de manière sectorielle (pour telle ou telle branche d'activité). Cependant, quelques États – en l'espèce, le Minnesota et la Californie – ont récemment adopté des lois plus complètes sur la protection de la vie privée ou envisagent de le faire. Le degré de protection varie d'un État à l'autre.

Approche à l'égard de la protection de la vie privée dans le secteur privé

Le gouvernement des États-Unis considère que les codes de conduite élaborés et mis en oeuvre par le secteur privé sont un moyen efficace de protéger la vie privée en ligne sans créer une bureaucratie susceptible d'étouffer la croissance du commerce électronique. Il encourage le développement des codes de conduite professionnels pour protéger la vie privée en ligne. Diverses agences gouvernementales, notamment le ministère du Commerce et la *Federal Trade Commission*, ont travaillé avec les associations professionnelles à l'élaboration de codes de conduite complets et applicables, mais le gouvernement des États-Unis ne privilégie officiellement aucun code de conduite en particulier. Parmi les rapports officiels et déclarations de responsables publics peuvent être cités :

- *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (juin 1995) de l'*Information Infrastructure Task Force* (IITF)⁷⁸ qui énonce un ensemble de principes de protection de la vie privée (*Privacy Principles*) reposant sur les Lignes directrices de l'OCDE.
- *Privacy and the National Information Infrastructure: Safeguarding Telecommunications-Related Personal Information* (octobre 1995)⁷⁹ de la *National Telecommunications and Information Administration* (NTIA) (qui fait partie du *Department of Commerce*) qui recommande que les fournisseurs de services de télécommunications et d'information appliquent des politiques de protection de la vie privée dans le cadre desquelles ils avertissent les utilisateurs de leurs pratiques à l'égard des informations et demandent à ces derniers leur consentement pour l'exploitation des informations à caractère personnel les concernant.
- *Options for Promoting Privacy on the National Information Infrastructure* (avril 1997)⁸⁰ de l'*Information Policy Committee* de l'IITF qui présente des options pour la mise en oeuvre de la protection de la vie privée en ligne, avec la création d'une entité fédérale chargée de la protection de la vie privée.

- *Individual Reference Services : A Report to Congress* (décembre 1997), rapport de la FTC qui analyse les avantages et les risques des bases de données de services de recherche utilisées pour localiser, identifier et vérifier l'identité des personnes. Ce rapport analyse également les principes d'autorégulation adoptés par les membres de cette industrie.
- *Elements of Effective Self-Regulation for Protection of Privacy* (janvier 1998)⁸¹ de la NTIA et du Department of Commerce, qui expose les actions que le secteur privé peut accomplir pour atteindre un degré acceptable de protection de la vie privée.
- *Privacy Online : A Report to Congress* (juin 1998) de la FTC qui souligne l'importance des principes d'avertissement, de choix, de sécurité et d'accès pour la protection de la vie privée, indique que des incitations substantielles sont nécessaires pour stimuler l'autorégulation et assurer une mise en œuvre généralisée des principes de base de protection de la vie privée, et recommande l'établissement d'une législation destinée à protéger la vie privée des enfants en ligne. Dans une déposition devant le *Subcommittee on Telecommunications, Trade and Consumer Protection* en juillet 1998, le Président de la FTC a recommandé que, dans l'hypothèse où un cadre d'autorégulation effectif ne serait pas en place sur une large base d'ici la fin de 1998, une législation soit élaborée qui impose des normes légales et autorise un organisme gouvernemental à en faire respecter l'application.⁸²
- Le Premier rapport annuel du Groupe de travail sur le commerce électronique du Gouvernement des États-Unis (1998), qui décrit les progrès accomplis dans l'instauration d'une autorégulation pour la protection de la vie privée et esquisse le rôle que devraient jouer les pouvoirs publics dans la protection de la vie privée.
- *Protection Consumers' Privacy : 2002 and Beyond*, observations du Président de la FTC, M. Timothy J. Muris, lors de la conférence Privacy 2001, Cleveland, OH, le 4 octobre 2001, www.ftc.gov/speeches/muris/privisp1002.htm.

Instruments d'autorégulation

Instruments concernant la protection de la vie privée dans les communications en ligne

Un certain nombre d'initiatives d'autorégulation ont été engagées aux États-Unis, notamment l'élaboration de codes de conduite sectoriels du secteur privé ainsi que l'établissement de systèmes de labels. Diverses associations pilotées par l'industrie se sont formées pour élaborer des codes de conduite du secteur privé visant à protéger la vie privée en ligne, notamment :

- La *Privacy Leadership Initiative (PLI)*, qui est composée de plus d'une vingtaine d'entreprises et associations, définit également les pratiques exemplaires (l'« étiquette ») pour l'échange d'informations personnelles entre les entreprises et les consommateurs.
- La *Network Advertising Initiative*, qui est un exemple de code de conduite sectoriel, a été créée par les plus importants publicitaires en ligne engagés dans le « profilage en ligne ». Ce code de conduite énonce les principes d'autorégulation destinés aux annonceurs en ligne pour protéger la vie privée des consommateurs dans le cadre des activités de profilage en ligne.

- L'*Information Technology Industry Council*⁸³ qui a adopté des principes pour la protection des données à caractère personnel dans le commerce électronique qui offrent une base permettant à chaque entreprise membre d'élaborer sa propre politique de protection de la vie privée ;⁸⁴
- L'*Interactive Services Association* a publié des « principes des procédures d'avertissement et de choix pour la collecte et la distribution d'informations en ligne par les exploitants de services en ligne » (juin 1997) à caractère non obligatoire, reposant sur un système d'avertissement et de faculté de refus (*opt out*) ;
- L'*Online Privacy Alliance*⁸⁵ (formée en juin 1998 par 50 entreprises et associations américaines en rapport avec l'Internet) a rédigé des *Guidelines for Online Privacy* (qui demandent aux membres de l'Alliance de souscrire aux Lignes directrices de l'OCDE et de recourir à des systèmes de label de protection de la vie privée administrés par des tiers, comme *TRUSTe* ou *BBBOnline*) ainsi qu'un ensemble de lignes directrices pour la protection de la vie privée des enfants ; et
- L'*American Electronics Association* a annoncé (juin 1998) des plans d'action pour l'autorégulation comprenant l'adoption d'un ensemble d'éléments pour la protection de la vie privée destinés à être mis en œuvre par ses entreprises membres.

Programmes de labels

De plus en plus utilisés par les cyberentreprises, les « programmes de labels » comme ceux de BBBOnline, TRUSTe et la *Direct Marketing Association* (DMA), ont pour fonction de garantir que les pratiques d'une entreprise sont conformes aux pratiques d'information équitable et que les cyberentreprises prévoient un mécanisme de règlement des différends. Les entreprises clientes de TRUSTe, BBBOnline et de la DMA se comptent aujourd'hui par milliers.

Autres initiatives

On peut aussi mentionner les autres initiatives d'autorégulation suivantes :

- L'élaboration par la *Direct Marketing Association*⁸⁶ de lignes directrices à caractère non obligatoire et des *Online Guidelines* basées sur les principes d'avertissement et de faculté de refus.
- La publication par la *Children's Advertising Review Unit* du *Council of Better Business Bureau* des « lignes directrices d'autorégulation pour la publicité destinée aux enfants »⁸⁷. Ces lignes directrices requièrent des « efforts raisonnables » pour avertir les parents et leur donner une faculté de choix quand des informations sont collectées en ligne auprès des enfants.
- La rédaction par la *Coalition for Advertising Supported Information and Entertainment* d'une déclaration sur les *objectifs de protection de la vie privée pour le marketing dans les médias interactifs*.

- L'accord par lequel l'*Individual Reference Services Group* (IRSG) s'est engagé auprès de la FTC en décembre 1997 à se conformer à un ensemble de principes (*IRSG Principles*) régissant les informations que fournissent les services de bases de données informatisées et qui peuvent être utilisées pour localiser les personnes ou déterminer ou vérifier leur identité. Les entreprises doivent se soumettre à un audit annuel effectué par des tiers, dont les résultats sont rendus publics.

FINLANDE

Constitution

L'article 10 de la *Constitution finlandaise* garantit à chaque citoyen le droit à la vie privée, l'honneur et l'inviolabilité du domicile. La Constitution contient également des dispositions détaillées relatives à la protection des données à caractère personnel. Ainsi, le secret de la correspondance, de la téléphonie ainsi que d'autres communications confidentielles est inviolable.

Législation

Lois horizontales

La *Loi sur les données à caractère personnel* (523/1999)⁸⁸, telle qu'amendée, constitue le cadre juridique de toutes les opérations de traitement de données à caractère personnel. Elle s'applique aux données à caractère personnel faisant l'objet d'un traitement informatisé et aux dossiers établis manuellement sur des personnes physiques dans les secteurs public et privé. Cette loi régleme la collecte, la correction, la divulgation, la conservation et l'utilisation des données à caractère personnel et confère aux personnes concernées le droit d'examiner l'information détenue à leur sujet et de demander que les erreurs qui s'y trouvent le cas échéant soient corrigées.

Il existe deux organismes de contrôle, l'*Ombudsman de la protection des données*⁸⁹ et le Comité pour la protection des données. Le premier fournit des orientations et des avis, supervise le traitement des données à caractère personnel et statue sur des questions concernant le droit d'accès et la rectification. Le second traite les questions de principe se rapportant à la loi, accorde des autorisations de traitement de données à caractère personnel ou de données sensibles et rend des décisions sur des questions de protection de données conformément aux dispositions de la loi.

La loi sur les données à caractère personnel prévoit des recours civils (par exemple, les maîtres de fichiers sont tenus d'indemniser les personnes concernées en cas d'utilisation illégale des données) ainsi que des sanctions pénales en cas de violations⁹⁰.

Autres lois comportant des dispositions de protection de la vie privée

Un certain nombre de lois finlandaises ont des incidences du point de vue de la protection des données et de la vie privée, notamment la *loi sur les statistiques*, la *loi sur le Centre de développement de la recherche médicale* et la *loi sur le statut et les droits des patients*. La *loi relative à la protection des données dans la vie professionnelle* prend en compte les principales questions de protection des données concernant la vie professionnelle en établissant des procédures relatives aux besoins de la vie professionnelle en particulier. La *loi sur la protection de la vie privée et la sécurité des données dans les télécommunications* contient des dispositions favorisant la sécurité des données des télécommunications publiques ainsi que la protection de la vie privée et des intérêts légitimes des abonnés et usagers des

télécommunications. Le Ministère des transports et des communications travaille à l'élaboration d'une nouvelle loi relative à la protection de la vie privée et aux communications électroniques qui devrait entrer en vigueur en octobre 2003. Cette loi est destinée à assurer la confidentialité et la protection de la vie privée dans les communications électroniques. Elle met en œuvre la directive vie privée et communications électroniques de l'UE, avec plusieurs amendements en droit interne.

Mise en œuvre de la directive de l'Union européenne

La loi sur les données à caractère personnel, adoptée pour transposer la directive de l'UE sur la protection des données, est entrée en vigueur le 1^{er} juin 1999.

Instruments d'autorégulation

La loi sur les données à caractère personnel contient des dispositions relatives aux codes de conduite sectoriels élaborés par les maîtres de fichiers ou leurs représentants. L'Ombudsman de la protection des données est habilité à vérifier si les codes de conduite sont conformes à la législation. Les règles relatives au commerce électronique⁹¹ ont été élaborées conjointement par la Chambre de commerce centrale de Finlande, l'Association finlandaise de marketing direct, la Fédération finlandaise du commerce ainsi que la Fédération finlandaise des communications et de la téléinformatique. Des codes de conduite ont également été élaborés à ce jour notamment pour le marketing direct.

FRANCE

Législation

Lois horizontales

La loi n° 78/17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* s'applique aux fichiers informatisés ou manuels concernant les personnes physiques dans le secteur public et dans le secteur privé. La loi 78/17 a été modifiée par la loi n° 94/548 qui institue un régime spécial pour le traitement des données personnelles de santé pour la recherche. Le *Code pénal* complète la loi 78/17.⁹²

La loi 78/17 établit un système central d'enregistrement qui est administré par une autorité de protection des données indépendante, la *Commission nationale de l'informatique et des libertés* (CNIL)⁹³. Cette autorité a pour mission d'informer et de conseiller le public sur les droits et obligations prévus par la loi, d'examiner les projets de traitement de données dans le secteur public préalablement à leur mise en œuvre, et de proposer des changements à la loi eu égard à l'évolution technologique. L'autorité agit d'initiative, sur plainte ou sur demande, effectue des investigations et veille à ce que les personnes concernées puissent exercer leur droit d'accès.

Aux termes de la loi 78/17, les auteurs de traitements ou transferts illicites de données nominatives sont passibles de peines d'amende ou d'emprisonnement⁹⁴. Les poursuites pénales en cas d'infraction à la loi peuvent être menées sur l'initiative de la personne concernée ou du ministère public.

Autres lois comportant des dispositions de protection de la vie privée

Parmi les lois sectorielles comportant des dispositions de protection de la vie privée, on peut notamment mentionner le *Code du travail*⁹⁵, et la loi sur la vidéosurveillance (1995)⁹⁶.

Mise en œuvre de la directive de l'Union européenne

Un rapport sur la transposition de la directive de l'Union européenne a été publié le 3 mars 1998 et un projet de loi est en préparation au *Ministère de la Justice*. Ce projet de loi sera examiné au niveau ministériel avant d'être soumis au *Parlement* français. La *Commission nationale consultative des droits de l'homme* et la CNIL seront consultées sur ce projet de loi.

Instruments d'autorégulation

Instruments concernant la protection de la vie privée dans les communications en ligne

La *Charte de l'Internet*⁹⁷ est une initiative d'autorégulation établie sur la base de la législation nationale. Cette Charte, destinée aux acteurs de l'Internet⁹⁸, établit un organisme de surveillance indépendant, le *Conseil de l'Internet*, ayant des attributions de conseil et de médiation. La Charte stipule notamment le droit d'utiliser des services d'anonymat et l'obligation, pour les acteurs de l'Internet d'informer les utilisateurs des données qui sont collectées.

Autres initiatives

Le *SEVPCD*, association professionnelle de la vente à distance, a rédigé un Code de déontologie conçu pour l'application de la loi 78/17⁹⁹. Seuls les membres qui se conforment à ces règles peuvent afficher l'emblème de l'Association et les infractions peuvent entraîner des procédures disciplinaires devant le Comité de surveillance de l'Association.

GRÈCE

Constitution

La Constitution grecque énonce les droits relatifs à la protection de la vie privée personnelle et familiale (article 9) et au secret (article 19).

Législation

Lois horizontales

La loi n° 2472/97 concernant la *protection des personnes à l'égard du traitement des données à caractère personnel*, adoptée le 26 mars 1997, transpose la directive de l'Union européenne¹⁰⁰. Cette loi s'applique aux fichiers informatisés ou manuels concernant les personnes physiques, dans le secteur public et dans le secteur privé. Elle établit aussi une *Autorité de protection des données* chargée de superviser le système d'enregistrement, de faire respecter la loi, de promouvoir l'adoption de codes sectoriels volontaires et de sanctionner les infractions¹⁰¹.

La loi donne aux personnes concernées le droit de s'informer sur leurs données à caractère personnel, d'y accéder, et de demander au tribunal la suspension de certaines opérations de traitement¹⁰². La loi prévoit une réparation, par la voie civile, des dommages causés en infraction à la loi¹⁰³, des sanctions administratives (telles que des amendes et l'annulation des licences de traitement de données)¹⁰⁴ ainsi que des sanctions pénales¹⁰⁵.

Autres lois comportant des dispositions de protection de la vie privée

La loi n° 2225/94 protège la liberté de correspondance et de communication.

Instruments d'autorégulation

En Grèce, il n'existe pas de codes de conduite spécifiquement consacrés à la protection de la vie privée, mais les codes déontologiques de l'*Association des journalistes* et de l'*Association grecque des banques* font mention de la protection de la vie privée.

HONGRIE

Constitution

La Constitution hongroise énonce le droit à la protection des données à caractère personnel (article 59).

Législation

Lois horizontales

La loi sur la Protection des données à caractère personnel et la divulgation des données d'intérêt public (1992)¹⁰⁶ s'applique aux fichiers informatisés ou manuels concernant les personnes physiques, dans le secteur public et le secteur privé, et elle instaure un système d'enregistrement limité. Un Commissaire parlementaire à la protection des données et à l'accès à l'information indépendant a été nommé conformément à la loi en 1995. Le Commissaire est chargé de surveiller l'application de la loi, d'enquêter sur les plaintes et de tenir le Registre de la protection des données.

La loi, qui contient les principes de base des Lignes directrices de l'OCDE, donne aux personnes concernées un certain nombre de droits sur leurs données à caractère personnel (notamment droits de correction ou de suppression de données)¹⁰⁷. La loi prévoit aussi des réparations (y compris une indemnisation) pour les infractions. On peut demander la réparation des préjudices en s'adressant au Commissaire¹⁰⁸ ou en intentant une action en justice¹⁰⁹.

Autres lois comportant des dispositions de protection de la vie privée

Il existe un certain nombre de lois sur des questions spécifiques contenant des dispositions relatives à la protection des données. Ces lois concernent notamment : le registre national, le traitement des informations dans les domaines de la recherche et de la vente directe, le traitement des données médicales, l'éducation, les archives, la police, la banque et la sécurité nationale.

Instruments d'autorégulation

Il existe divers exemples d'initiatives d'autorégulation, notamment la coopération instaurée entre les entreprises de vente directe et les règles adoptées par exemple par l'Association nationale hongroise des journalistes. Le Bureau du Commissaire pour la protection des données propose des conseils professionnels à ceux qui sont chargés d'élaborer des règles de déontologie.

IRLANDE

Constitution

La Constitution irlandaise reconnaît le droit à la protection de la vie privée¹¹⁰.

Législation

Lois horizontales

Le *Data Protection Act 1988* (loi sur la protection des données) concerne les données informatisées à caractère personnel relatives aux personnes physiques et elle établit un système d'enregistrement limité applicable à certaines catégories de responsables de fichier (secteur public, détenteurs de données sensibles, institutions financières et organisations menant des activités de vente directe, de recouvrement de créances ou de renseignements sur la solvabilité des emprunteurs).

La loi institue un *Commissaire à la protection des données* nommé par le gouvernement. Le Commissaire met la loi à exécution en enquêtant sur les plaintes, en poursuivant les auteurs d'infraction, en supervisant l'enregistrement et en encourageant l'élaboration de codes de conduite sectoriels. Les décisions du Commissaire à la protection des données peuvent être contestées devant les tribunaux.

La loi établit des principes de protection des données qui doivent être respectés pour tous les traitements, qu'il y ait lieu ou non à l'enregistrement. La violation d'un de ces principes ne constitue pas en elle-même un délit pénal mais, si le Commissaire examine une plainte et émet une mise en demeure, l'inexécution sans raison valable devient un délit. La loi institue des délits pénaux comme la divulgation non autorisée¹¹¹. Les personnes concernées peuvent intenter une action civile pour obtenir une indemnisation des dommages résultant d'une infraction à la loi.

Autres lois comportant des dispositions de protection de la vie privée

L'Irlande a aussi une législation spécifique concernant les données statistiques, ainsi que des règlements relatifs à la protection de la vie privée et des données à caractère personnel.

Mise en œuvre de la directive de l'Union européenne

Le texte provisoire d'un projet de loi visant à transposer la directive de l'Union européenne a été soumis au bureau de l'Attorney-General et sera présenté au Parlement avant la mi-juillet 1999. Ce texte fait suite au document de consultation intitulé *Consultation Paper on Transposition into Irish Law* publié par le ministère de la Justice (*Department of Justice, Equality and Law Reform*, novembre 1997).

Instruments d'autorégulation

Le Code de conduite¹¹² de l'*Irish Direct Marketing Association* (IDMA) sert de guide pour l'application du *Data Protection Act* à la vente directe. S'agissant de la mise en œuvre, une personne doit être désignée dans l'entreprise pour veiller au respect du code et effectuer des contrôles, et les plaintes peuvent être adressées au Comité de l'IDMA qui a le pouvoir d'exclure l'entreprise de l'Association.

Les codes de conduite peuvent être validés par le Parlement irlandais, ce qui leur donne force de loi.

ISLANDE

Législation

Lois horizontales

La législation islandaise régissant la protection des données (*Loi n° 121 concernant l'enregistrement et le traitement des données à caractère personnel*, 28 décembre 1989) s'applique aussi bien au secteur public qu'au secteur privé. Cette législation couvre les fichiers informatisés ou manuels concernant les personnes physiques ou morales. Elle établit aussi un système central d'enregistrement supervisé par la *Commission islandaise de protection des données*. La Commission traite aussi les cas d'infraction à la Loi¹¹³ et délivre les autorisations pour le traitement de données à l'étranger.

Les personnes concernées ont le droit d'accéder à leurs données et elles peuvent exiger une rectification ou la suppression de ces données à caractère personnel¹¹⁴. Elles peuvent aussi demander que leur nom soit rayé des listes de publipostage¹¹⁵. En cas de litige concernant les droits d'une personne, l'affaire peut être portée devant la Commission de protection des données. La Commission peut émettre des ordres en cas d'atteinte aux droits des personnes concernées¹¹⁶.

La loi de 1989 établit des sanctions pénales pour les infractions à certaines dispositions¹¹⁷.

ITALIE

Législation

La loi sur la protection des données n° 675/1996 (qui transpose en droit interne la directive 95/46 de l'UE) couvre les données à caractère personnel faisant l'objet d'un traitement automatisé ou manuel se rapportant aux personnes physiques et morales dans les secteurs public et privé. La loi prévoit une rigoureuse protection des données sensibles et notamment des dispositions concernant le traitement de ces données par les organismes publics (décret-loi n° 135 du 11.05.1999). Elle précise les situations dans lesquelles le traitement peut être considéré comme servant l'intérêt général et est par conséquent automatiquement autorisé en vue de cette finalité. S'agissant des maîtres de fichiers privés, la légalité du traitement des données sensibles repose sur une autorisation expresse délivrée par le *Garante* — le consentement écrit de la personne concernée étant nécessaire mais non suffisant. Depuis 1997, ce type de traitement est autorisé par le *Garante* au moyen d'une « autorisation générale » définissant la portée dudit traitement.

Le décret n° 281 du 30.07.1999 comprend des dispositions visant expressément le traitement des données à caractère personnel à des fins chronologiques, statistiques et de recherche scientifique. Il insiste sur le rôle des codes de conduite et d'éthique. Le décret n° 282/1999 a également été promulgué pour réglementer le traitement des données à caractère médical par les organismes de santé publique, ou les organismes ou professionnels de santé qui exercent leurs fonctions dans le cadre d'un accord conclu avec les services nationaux de santé ou en bénéficiant d'une reconnaissance officielle de ces services.

S'agissant des mesures de sécurité, des règles à cet égard ont été énoncées dans le décret n° 318/1999, qui fixe les normes de sécurité minimales applicables au traitement des données à caractère personnel. Différentes mesures sont prévues, selon que des moyens électroniques ou automatisés sont utilisés pour le traitement ainsi que selon les types de données (les données sensibles font l'objet d'une attention particulière).

Le décret n° 467/2001 a été promulgué pour aligner plus étroitement le droit italien sur certains principes de la directive. Ce décret simplifie et rationalise les conditions à respecter pour le traitement des données et renforce les mesures de protection s'appliquant aux personnes concernées sur la base de l'expérience acquise dans la mise en œuvre de la loi sur la protection des données. Les principales questions prises en compte dans cette loi sont le principe de la mise en balance des intérêts, la question de la vérification préalable, la simplification des obligations de notification ainsi que le droit applicable. Le décret insiste sur l'adoption de nouveaux codes de conduite et pratiques professionnelles, qui se sont révélés relativement efficaces pour pleinement mettre en œuvre les principes énoncés dans la loi sur la protection des données ainsi que dans les recommandations du Conseil de l'Europe concernant plusieurs secteurs, lesquels ont tous été expressément mentionnés conformément au principe de représentation adéquate. Le décret n° 467/2000 modifie également la méthode de sanctions établie dans la loi n° 675/1996, en modifiant la nature de quelques sanctions et en prévoyant dans une certaine mesure la reconnaissance de la « repentance » d'un maître de fichiers en cas de violation des règles de sécurité minimale. De plus, les cas graves de fausse déclaration et/ou communication aux autorités de contrôle sont désormais passibles de sanctions pénales. Le décret 171/1998 a été complété par des dispositions expresses qui transposent la directive 97/66 de la CE dans le droit italien. Ces dispositions concernent notamment les modalités selon lesquelles d'autres méthodes de paiement possibles seraient effectivement proposées, de façon à garantir l'anonymat de l'utilisateur, ainsi que l'obligation pour les prestataires de services de télécommunications de dûment informer le public sur les services d'identification du numéro du demandeur et de veiller à ce qu'il soit possible d'annuler la neutralisation de la fonction d'identification du demandeur pour les appels d'urgence.

En application de l'article 28 de la directive 95/46 de la CE, le *Garante per la protezione dei dati personali*, doit contrôler l'application des dispositions adoptées pour mettre en œuvre la directive. Le *Garante* est également chargé de suivre l'application des conventions de Schengen, Europol, Eurodac et CIS.

Les tâches les plus importantes du *Garante* sont les suivantes : vérifier si les opérations de traitement de données sont effectuées conformément à la législation en vigueur et à la notification pertinente ; recevoir des rapports et des plaintes ; encourager, dans les catégories concernées et en conformité avec le principe de représentation, l'élaboration de codes d'éthique et de conduite pour certains secteurs et contribuer à l'adoption et à la mise en application de ces codes ; informer le gouvernement de la nécessité de légiférer en tant que de besoin selon l'évolution du secteur. En outre, le Premier Ministre et chacun des ministres sont tenus de consulter le *Garante* lorsqu'ils élaborent des règlements et mesures administratives concernant la protection des données.

La procédure de dépôt de plainte auprès du *Garante* — en vertu de l'article 29 de la loi sur la protection des données — est entrée en vigueur en 1999 (d.P.R. n° 501/1998). Cette démarche peut se substituer à une poursuite judiciaire et permet aux personnes concernées d'obtenir des décisions rapides. Ce type de plainte ne peut être déposée qu'en cas d'impossibilité partielle ou totale d'exercer les droits conférés aux personnes concernées par l'article 13 de la loi sur la protection des données (droits d'accès, de rectification, d'information, d'effacement, etc.).

Instruments d'autorégulation

L'Autorité a ainsi participé à l'élaboration des codes de conduite suivants :

- Le Code de conduite pour le traitement des données personnelles dans l'exercice d'activités journalistiques a été rédigé par le Conseil national de la presse en collaboration avec l'Autorité de protection des données. L'élaboration de ce code a permis de prendre des dispositions précises à l'égard des modalités simplifiées – qui portent également sur l'information des personnes concernées au moment de la collecte des données – définies pour le traitement des données personnelles dans l'exercice d'activités journalistiques. Le Code de conduite, qui s'applique au traitement des données personnelles à des fins chronologiques, vise à faire en sorte que les données personnelles obtenues dans le cadre d'une recherche rétrospective, de l'exercice du droit de recherche et d'information, ainsi que des activités liées aux archives soient utilisées dans le respect des droits, des libertés fondamentales et de la dignité des personnes concernées, et en particulier du droit à la vie privée et à l'identité personnelle.
- Le Code de conduite et de pratique professionnelle applicable au traitement des données personnelles à des fins statistiques et de recherche scientifique dans le cadre du système national de statistiques.
- Les codes de conduite pour les avocats de la défense et les détectives privés sont en voie d'achèvement.

Seront également adoptés sous peu les codes suivants en application de l'article 20 du décret législatif n° 467/2001, en ce qui concerne le traitement de données personnelles :

1. Qui est effectué par un prestataire de services de communication et d'information offerts sur des réseaux électroniques.
2. Qui est nécessaire à des fins de sécurité sociale dans le cadre de la relation employeur/employé.
3. Qui est effectué en vue d'envoyer de la documentation publicitaire et/ou de procéder à des activités de vente directe.
4. Qui est effectué à des fins d'information commerciale.
5. Dans le cadre de systèmes d'information appartenant à des entités privées.
6. Contenus dans des archives, registres, listes, fichiers ou documents détenus par des organismes publics.
7. Qui est effectué à l'aide de dispositifs d'acquisition automatisée d'images.

Le respect des dispositions énoncées dans les codes précités constituera une condition fondamentale de la légalité du traitement. Les codes seront publiés dans le *Journal officiel* sous la responsabilité du *Garante* et seront annexés au texte unifié des dispositions relatives à la protection des données.

JAPON

Législation

Lois gouvernant le secteur public

La Loi sur la protection des données personnelles traitées par ordinateur détenues par des organes administratifs (1988) couvre les données informatisées concernant les personnes physiques. La Loi suit d'une manière générale les Lignes directrices de l'OCDE. Le ministère de la Gestion publique, de l'Intérieur, des Postes et des Télécommunications contrôle l'application de la loi, qui oblige les organismes publics à publier des avis énumérant les fichiers qu'ils détiennent et confère aux personnes concernées le droit d'accès aux données à caractère personnel recueillies à leur sujet.

Le Cabinet propose un nouveau texte, couvrant les données traitées par ordinateur et manuellement, qui permet aux personnes concernées d'exercer plusieurs droits à l'égard des données recueillies à leur sujet (accès, correction et suspension d'utilisation).

Approche à l'égard de la protection de la vie privée dans le secteur privé

Des principes de base destinés à promouvoir la société avancée de l'information et des télécommunications (Cabinet du Premier Ministre, 1998) ont été établis qui définissent en matière de vie privée un certain nombre d'orientations selon lesquelles *i*) le secteur privé devrait prendre l'initiative de formuler des lignes directrices, des systèmes d'enregistrement et des systèmes de labellisation propres à chaque branche d'industrie ou d'activité. *ii*) en revanche, les réglementations gouvernementales concernant des entités qui traitent des données hautement confidentielles, comme les données financières et médicales personnelles dont la divulgation peut être préjudiciable, doivent être prises en considération. En résumé, le Gouvernement sera tenu de promouvoir les efforts indépendants dans le secteur privé et aussi de réexaminer la situation, compte tenu des réglementations légales. Le Gouvernement doit aussi faire le nécessaire pour encourager les entreprises à indiquer aux consommateurs la façon dont elles protègent les données de caractère personnel.

Le rapport intitulé « Réunion de consultation pour la protection et l'utilisation des données personnelles de crédit » (Ministère du commerce international et de l'industrie – MITI – et Ministère des finances, 1998) indiquait le besoin d'une réglementation juridique destinée à protéger les données personnelles de crédit. Le rapport du Groupe d'étude sur la protection de la vie privée dans le secteur des télécommunications (Ministère des Postes et Télécommunications – MPT, 26 octobre 1998) signalait également le besoin d'une assise juridique pour donner toute leur efficacité aux Lignes directrices pour la protection des données de caractère personnel dans les entreprises de télécommunications. Le gouvernement japonais encourage aussi activement l'adoption de codes de conduite par le secteur privé (voir ci-dessous).

En octobre 2000, le Comité législatif pour la protection de l'information personnelle, qui relève du Centre pour la promotion d'une société avancée de l'information et des télécommunications, a publié une ébauche de législation fondamentale pour la protection de l'information personnelle. Dans le prolongement de cette législation, le Secrétariat du Cabinet propose le projet de loi sur la protection de l'information personnelle, qui couvre l'ensemble du secteur privé et confère aux personnes concernées plusieurs droits sur l'information qui les concerne (notamment l'accès aux données, la correction des données et la suspension de l'utilisation de ces données).

Réglementation des autorités locales

Il existe au Japon un grand nombre d'Ordonnances promulguées par les autorités locales qui garantissent la protection de la vie privée en ce qui concerne les données manuelles ou informatisées. La plupart de ces Ordonnances ne s'appliquent qu'aux administrations publiques locales mais quelques-unes s'étendent au secteur privé¹¹⁸.

Instruments d'autorégulation

En mars 1997, le ministère du Commerce international et de l'Industrie (*Ministry of International Trade and Industry*, MITI) a publié des Lignes directrices concernant la protection des données personnelles informatisées dans le secteur privé¹¹⁹. Ces Lignes directrices du MITI s'appliquent aux données à caractère personnel traitées électroniquement et elles visent à servir de modèle pour les codes sectoriels. Elles tiennent compte des Lignes directrices de l'OCDE ainsi que de la directive de l'Union européenne. D'après ces Lignes directrices du MITI, un responsable devrait être désigné dans chaque organisation pour veiller à leur application¹²⁰. Un « Système d'attribution de marque de protection de la vie privée », certifiant que les entreprises respectent les codes industriels imposant le maintien de niveaux appropriés de protection de la vie privée, a été mis en place par le Centre japonais pour le développement du traitement de l'information en avril 1998. Ce système garantit aussi que les consommateurs peuvent aisément distinguer entre les différents niveaux de protection des données de caractère personnel assurés par les entreprises.

L'*Electronic Network Consortium*¹²¹ (ENC) a publié des Lignes directrices pour la protection des données personnelles (décembre 1997) qui s'inspirent des Lignes directrices de l'OCDE. Elles s'appliquent à quiconque manie des données à caractère personnel dans les réseaux électroniques et elles visent à encourager les fournisseurs de service à adopter une approche uniforme à l'égard de la gestion et de la protection des données personnelles.

Les associations d'entreprises de commerce électronique ont aussi rédigé des codes de conduite pour la protection de la vie privée. La *Cyber Business Association*, en consultation avec le MPT, a publié un code volontaire intitulé *Guidelines for Protecting Personal Information in Cyber Business* (décembre 1997). L'*Electronic Commerce Promotion Council* (ECOM)¹²² a aussi formulé des Lignes directrices. Le Groupe de travail de l'ECOM sur la protection de la vie privée a publié des Lignes directrices (*Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector*, mars 1998) basées sur celles du MITI, qui contiennent des dispositions spéciales concernant les enfants, exigeant le consentement des parents ou tuteurs. Elles visent à servir de modèle pour chaque entreprise.

Concernant l'autorégulation dans la branche des fournisseurs de service Internet, la *Telecom Services Association* (TELESA) a aussi rédigé un Code de conduite type qui contient des dispositions relatives à la protection de la vie privée et des données à caractère personnel.¹²³

En avril 1998, la *Japan Data Communications Association* a lancé un système de délivrance de labels pour certifier que les opérateurs de télécommunications et les fournisseurs de service assurent une protection adéquate de la vie privée dans leurs opérations de traitement de données de caractère personnel.

Le MPT a établi en 1991 des « Lignes directrices pour la protection des données de caractère personnel dans les activités de télécommunications », qui ont été révisées en 1998. Ces Lignes directrices énoncent cinq principes de base, que doivent respecter les opérateurs de télécommunications et les fournisseurs de service Internet (limitation de la collecte, de l'utilisation et de la divulgation, garanties en matière de sécurité, participation individuelle et responsabilité), ainsi que six autres clauses plus particulièrement axées sur les questions propres au secteur des télécommunications (données sur le trafic,

facturation détaillée, identification de la ligne appelante, etc.). De même, en 1998, la loi sur les entreprises de télécommunications a été modifiée et un système de réclamation a été mis en place. Les utilisateurs peuvent enregistrer leurs plaintes et leurs demandes auprès du MPT concernant les redevances sur les services de télécommunications, les autres modalités appliquées ou la façon dont ces services sont exploités, notamment en ce qui concerne le traitement des données de caractère personnel des utilisateurs. Ce système devrait servir de modèle pour permettre aux particuliers d'obtenir réparation dans les cas de violation de la vie privée. Le MPT a établi un certain nombre d'autres lignes directrices, notamment : les « lignes directrices pour la protection des informations à caractère personnel de l'appelant dans les services d'identification de l'appelant » (1996) et les « lignes directrices pour la protection des informations à caractère personnel de l'abonné dans la diffusion audiovisuelle » (1996).

On peut aussi mentionner d'autres initiatives d'autorégulation concernant la protection de la vie privée comme celles du *Centre for Financial Industry Information Systems*, qui a publié des Lignes directrices sur la protection des données personnelles à l'usage des institutions financières basées sur les Lignes directrices de l'OCDE.

En mars 1999, le ministère du Commerce international et de l'Industrie a promulgué une norme industrielle japonaise (JIS ou *Japanese Industrial Standard*) intitulée « Critères de contrôle de la protection des informations de caractère personnel » afin de normaliser le niveau de protection des données de caractère personnel dans les entreprises.

LUXEMBOURG

Législation

Lois horizontales

La loi réglementant l'utilisation des données nominatives dans les traitements informatiques (1979)¹²⁴ s'applique aux fichiers informatisés ou manuels concernant les personnes physiques et les personnes morales, détenus aussi bien dans le secteur public que dans le secteur privé. La *Commission consultative à la protection des données* travaille sous les auspices du Ministre compétent en matière de banques de données et elle a une fonction de conseil. Le Ministre reçoit aussi l'assistance d'une *Autorité de contrôle*¹²⁵. Le Ministre peut saisir le ministère public des infractions à la législation de protection de la vie privée.

La loi de 1979 établit des sanctions pénales (emprisonnement ou amendes) pour les infractions à ses dispositions¹²⁶.

Autres lois comportant des dispositions de protection de la vie privée

Un certain nombre de réglementations sectorielles ont été établies en application de la loi, par exemple concernant les fichiers de police et les fichiers médicaux¹²⁷.

Mise en œuvre de la directive de l'Union européenne

Un projet de loi transposant la directive de l'Union européenne a été rédigé¹²⁸. Il a été présenté à la Chambre des Députés le 8 octobre 1997.

MEXIQUE

Constitution

Les articles 6 et 7 de la *Constitution mexicaine* garantissent le droit à l'information. L'article 16 déclare que les communications privées sont inviolables et que la loi établira des sanctions pénales pour les actes portant atteinte à la liberté et au secret de ces communications.

Législation

Lois fédérales

Le *Code pénal du District fédéral* établit des sanctions pour les atteintes au respect de la vie privée commises par les fonctionnaires publics concernant les informations à caractère personnel collectées et tenues par les autorités publiques¹²⁹.

NORVÈGE

Législation

Lois horizontales

La législation norvégienne de la protection des données personnelles [Loi du 14 avril 2000 n°31 concernant le traitement des données personnelles (loi sur les données personnelles)] s'applique aux secteurs public et privé et porte sur les fichiers informatisés ou manuels concernant les personnes physiques et morales. Des modifications ultérieures de cette loi régissent le publipostage, le démarchage par téléphone et les renseignements sur les emprunteurs dans le cadre du crédit à la consommation. La loi couvre également la vidéosurveillance et il existe aussi deux autres textes juridiques visant expressément la protection des données personnelles : la loi n°24 du 18 mai 2001 sur les systèmes de classement de données médicales personnelles et le traitement des données médicales personnelles, ainsi que la loi n°66 du 16 juillet 1999 sur le système d'information de Schengen (SIS).

La loi établit un système central d'enregistrement, administré par une *Inspection des données (datatilsynet)*¹³⁰, qui veille à l'exécution de la loi, en effectuant notamment des inspections sur les pratiques des entreprises. Le Tribunal d'appel en matière de vie privée reçoit les appels interjetés de décisions de l'Inspection des données en vertu de la loi n°31 du 14 avril 2000 concernant le traitement des données personnelles (loi sur les données personnelles), article 42, paragraphe 4. Le Tribunal est une instance administrative indépendante qui relève du Roi et du Ministère.

Aux termes de la loi, une personne a le droit d'inspecter les données qui la concernent, de demander que des corrections y soient apportées et de s'opposer à ce que son nom soit utilisé dans la distribution publicitaire. Il existe aussi une protection spéciale pour les données sensibles. Les auteurs d'infractions délibérées ou par négligence aux conditions d'une licence, ou aux dispositions de la loi, sont passibles d'une peine d'amende ou d'emprisonnement. Les personnes qui ont subi de ce fait un préjudice ont le droit à recevoir une indemnisation de l'auteur de l'infraction.

Autres lois comportant des dispositions de protection de la vie privée

La législation norvégienne comporte de nombreuses dispositions concernant la protection de la vie privée, avec notamment la loi sur les télécommunications, qui vise la protection de la vie privée dans le secteur des télécommunications, ainsi que les règles du secret professionnel figurant dans la loi sur l'administration publique et la loi sur les fichiers nationaux, qui l'une et l'autre limitent l'utilisation des données de caractère personnel par les pouvoirs publics.

Autres instruments de protection des données de caractère personnel

L'Accord de base entre la Confédération norvégienne des syndicats (LO) et la Confédération des entreprises et industries norvégiennes (NHO) contient des dispositions visant la protection des données de caractère personnel. L'Accord prévoit des dispositions particulières concernant le stockage et l'utilisation des données de caractère personnel dans les entreprises privées.

Mise en œuvre de la directive de l'Union européenne

La directive 95/46 a été intégralement transposée dans le droit norvégien.

Instrument d'autorégulation

La loi sur les fichiers de données de caractère personnel a proposé que les entreprises et les secteurs d'activité élaborent leurs propres codes de conduite concernant les données de caractère personnel. A cet égard, la Commission s'est référée à l'article 27 de la directive de l'UE sur la protection des données et aux Lignes directrices de l'OCDE de 1980.

NOUVELLE-ZÉLANDE

Législation

Lois horizontales

La *Privacy Act 1993* s'applique aux « informations personnelles » informatisées ou manuelles détenues par presque toutes les organisations des secteurs public ou privé en Nouvelle-Zélande. Le noyau de cette loi est un ensemble de 12 principes intitulés *Information Privacy Principles* (IPP) qui ont pour base les Lignes directrices de l'OCDE. Cette loi énonce aussi des règles concernant le recoupement de données entre les organismes publics¹³¹.

La loi établit un Commissaire à la protection de la vie privée (*Privacy Commissioner*)¹³², officier de la Couronne indépendant, qui a des pouvoirs d'enquête et de médiation concernant les plaintes. Le Commissaire peut publier des *Codes de pratique* sectoriels qui peuvent être mis à exécution de la même manière que les IPP¹³³.

Ni les IPP ni les Codes de pratique spécifiques ne créent des droits directement exécutoires. Une infraction supposée peut constituer la base d'une plainte déposée auprès du Commissaire, qui a d'importants pouvoirs d'enquête et de conciliation. Les plaintes qui ne peuvent se régler à l'amiable sont transmises à un *Complaints Review Tribunal*¹³⁴ qui a de larges pouvoirs pour ordonner réparation.

Autres lois comportant des dispositions de protection de la vie privée

Parmi les lois sur des sujets spécifiques comportant des dispositions de protection de la vie privée, on peut mentionner l'*Official Information Act 1982* (informations officielles), le *Local Government Official Information and Meetings Act 1987* (informations des administrations locales), l'*Electoral Act 1993* (loi électorale) et le *Domestic Violence Act 1995* (violence domestique).

Instruments d'autorégulation

Concernant l'industrie de l'Internet, l'*Internet Society of New Zealand* a élaboré un code à l'usage des fournisseurs de service Internet (*Internet Service Provider Code of Practice*)¹³⁵.

La *Privacy Act* prévoit aussi l'établissement de Codes de pratique ayant force de loi. Un Code peut fixer des procédures de conformité et de plainte et peut être plus ou moins exigeant que les IPP mais, dès lors que le Commissaire à la protection de la vie privée l'a approuvé, il se substitue à ces principes pour l'organisme, le type d'informations, l'activité ou l'association professionnelle considérés. Le *Health Information Privacy Code 1994*¹³⁶ (santé) et le *Justice Sector Unique Identifier Code 1998*¹³⁷ (justice) sont des exemples de codes créés en vertu de cette loi.

PAYS-BAS

Constitution

L'article 10 de la *Constitution des Pays-Bas* garantit un droit constitutionnel à la protection de la vie privée.

Législation

Lois horizontales

Le *Wet bescherming persoonsgegevens* (loi sur la protection des données)¹³⁸ s'applique aux secteurs public et privé et porte sur les fichiers faisant l'objet d'un traitement informatisé ou manuel. L'autorité de contrôle indépendante est le *College bescherming persoonsgegevens* (Autorité de protection des données), qui a pour tâche de conseiller le gouvernement sur les projets de législation et autres textes réglementaires, d'approuver les codes de conduite, de recevoir les plaintes et de mener les enquêtes, et de tenir un registre public des notifications.

La Loi confère aux personnes concernées plusieurs droits, notamment le droit d'accès aux données, de rectification, d'effacement ou de blocage de ces données. Les personnes concernées ont le droit de s'opposer au traitement. Si le maître de fichier refuse d'accéder à la demande d'une personne concernée, celle-ci peut choisir parmi plusieurs options. Si le maître de fichier est un organisme public, la personne concernée devrait déposer une objection auprès de lui, puis porter l'affaire en appel devant le tribunal administratif. Si le maître de fichier est un organisme privé, elle peut saisir le juge cantonal. Mais avant d'engager une action, la personne concernée peut déposer une plainte auprès de l'Autorité de protection des données, laquelle a le pouvoir d'enquêter, sur demande et de sa propre initiative, et dispose de pouvoirs administratifs exécutoires. La loi sur la protection des données prévoit également des sanctions pour certaines infractions.

Autres lois comportant des dispositions de protection de la vie privée

La législation sectorielle relative à la protection de la vie privée se présente sous deux formes. On distingue d'une part les lois d'application sectorielle qui créent un régime complet de protection de la vie privée et excluent l'application de la loi générale (loi sur la protection des données). Entrent par exemple dans cette catégorie de législation les textes concernant les fichiers de police [*Wet Politierregisters*, Wpolr, Loi sur les registres de police (1990)], la loi sur les bases de données municipales (fichiers personnels) [*Wet gemeentelijke basisadministratie persoonsgegevens* (1994)] et la loi sur la documentation judiciaire [*Wet justitiële documentatie* (1955)].

Il existe par ailleurs des lois d'application sectorielle qui énoncent un certain nombre de règles concernant la protection de la vie privée, tandis que la loi sur la protection des données demeure applicable là où le texte d'application sectorielle ne s'applique pas. Entre dans cette catégorie la Loi concernant les données médicales [*Wet geneeskundige behandelingsovereenkomst*, Wgbo, Loi sur les informations médicales (1995)], la Loi générale sur la sécurité sociale [*Algemene bijstandswet*, (1995)] et la Loi relative au registre du commerce [*Handelsregisterwet* (1996)].

Mise en œuvre de la directive de l'Union européenne

La directive 95/46/CE a été transposée dans le droit néerlandais par une loi du 6 juillet 2000 (*Wet bescherming persoonsgegevens*) entrée en vigueur le 1^{er} septembre 2001, qui remplace l'ancienne loi sur la protection des données (*Wet persoonsregistraties*), laquelle remontait au 28 décembre 1988. Le même jour, l'autorité de contrôle, la *Registratiekamer* a changé de nom pour devenir le *College bescherming persoonsgegevens* (CBP).

La nouvelle loi diffère sur certains points de la précédente loi sur la protection des données, mais il existe en général une nette continuité entre les deux. La nouvelle loi s'applique au traitement des données de caractère personnel par des procédés automatiques et manuels. Elle comporte des dispositions sur les questions suivantes : conditions du traitement légal de données de caractère personnel, codes de conduite des organisations, communication d'informations aux personnes concernées et droits de ces personnes, sensibilisation des organismes de contrôle et du grand public aux questions de traitement des données. La loi couvre aussi les questions de protection légale, de responsabilité du maître du fichier, les transferts internationaux de données et les relations avec les autres textes législatifs. Le rôle de l'Autorité de protection des données est resté dans une large mesure le même, bien qu'il ait été complété par de nouveaux pouvoirs d'exécution.

Tout nouveau traitement effectué depuis le 1^{er} septembre 2001 doit être conforme aux nouvelles dispositions. Une période de transition d'un an, qui s'est terminée le 1^{er} septembre 2002, était prévue pour les traitements en cours.

En ce qui concerne la transposition de la directive 97/66/CE de l'UE, le principal texte contenant des règles sectorielles sur cette question est la loi sur les télécommunications du 19 octobre 1998 (*Telecommunicatiewet*)¹³⁹. Cette loi transpose en partie la directive dans le droit néerlandais. Les éléments de la directive qui restent à mettre en œuvre le seront en même temps que sera transposée la directive 2002/58/CE. L'Autorité néerlandaise de protection des données s'est prononcée sur un projet de révision de la loi sur les télécommunications en décembre 2002.

Instruments d'autorégulation

L'Autorité de protection des données s'est déclarée nettement en faveur de l'autorégulation et estime que les autorités publiques comme les organismes privés sont d'importants acteurs dans le domaine de la protection des données. L'ancienne loi comme la nouvelle contiennent des dispositions relatives à l'élaboration de codes de conduite pour mettre en œuvre l'autorégulation, avec la possibilité de solliciter l'approbation de l'Autorité de protection des données. Douze codes de conduite ont été officiellement approuvés en vertu de l'ancienne loi sur la protection des données. Ces codes, qui couvrent les principaux secteurs comme la banque, l'assurance, le marketing direct, la santé, les organismes de notation de crédit et la recherche pharmaceutique, suscitent encore un très grand respect. La plupart des codes en vigueur sont en cours de révision pour être adaptés aux dispositions de la nouvelle loi sur la protection des données. Les codes de conduite pour le secteur pharmaceutique et le secteur financier ont été approuvés en vertu de cette loi.

La loi néerlandaise sur la protection des données prévoit également la possibilité de nommer un responsable de la protection des données dans une entreprise pour superviser le traitement des données à caractère personnel. Cette personne bénéficie d'une protection juridique qui lui garantit l'indépendance nécessaire. Depuis septembre 2001, une centaine d'organisations – ministères, municipalités, écoles, hôpitaux, ainsi que grandes et moyennes entreprises – ont nommé des responsables de la protection des données.

POLOGNE

Constitution

L'article 51 de la *Constitution polonaise* garantit des droits à la protection des données à caractère personnel¹⁴⁰.

Législation

Lois horizontales

La *Loi sur la protection des données personnelles* (1997)¹⁴¹ s'applique aux fichiers manuels et électroniques et est conforme à la Convention 108 et à la directive de l'Union européenne. L'autorité de protection des données établie dans le cadre de cette loi est l'*Inspection générale de la protection des données personnelles*. La loi établit un certain nombre de sanctions pénales (amendes ou emprisonnement)¹⁴².

Autres lois comportant des dispositions de protection de la vie privée

Un Décret du *Ministère de la Santé* de 1993 contient des dispositions protégeant les données médicales.

PORTUGAL

Constitution

L'article 35 de la *Constitution portugaise* garantit des droits constitutionnels à la protection de la vie privée.

Législation

Lois horizontales

La *Loi sur la protection des données personnelles* (1991)¹⁴³ concerne les données informatisées relatives aux personnes physiques et est applicable aussi bien au secteur public qu'au secteur privé ; elle institue un système central d'enregistrement. La loi crée aussi une *Commission nationale de protection des données personnelles informatisées* (*Comissao Nacional de Proteccao de Dados Pessoais Informatizados*). Cette Commission est chargée d'administrer le système d'enregistrement, d'examiner les plaintes¹⁴⁴ et de faire respecter les droits à la protection de la vie privée garantis par la loi et la Constitution. La Commission surveille aussi le recoupement des fichiers de données à caractère personnel informatisés et son autorisation est requise pour les flux transfrontières.

La loi crée un droit d'accès pour les personnes concernées ainsi qu'un droit de rectification ou suppression¹⁴⁵. Les infractions à la loi¹⁴⁶, ainsi qu'à la Constitution, sont des délits pénaux.

Autres lois comportant des dispositions de protection de la vie privée

Il existe au Portugal un certain nombre de lois et réglementations contenant des dispositions pour la protection des données, notamment : la loi sur la délinquance informatique (1991)¹⁴⁷, les réglementations établissant des institutions comme le registre des non-donneurs d'organes humains¹⁴⁸ ou le Centre des cartes d'identité¹⁴⁹, et les réglementations régissant les bases de données exploitées par la Gendarmerie¹⁵⁰, les Services des affaires frontalières et étrangères¹⁵¹ et la Police criminelle¹⁵².

Mise en œuvre de la directive de l'Union européenne

En septembre 1997, il a été proposé un certain nombre de changements à l'article 35 de la Constitution pour qu'il soit en accord avec les principes de la directive de l'Union européenne. En outre, le gouvernement a approuvé le texte d'une nouvelle loi de protection des données qui est actuellement soumise au Parlement portugais.

RÉPUBLIQUE SLOVAQUE

Législation

Lois horizontales

La Convention n°108 ainsi que ses annexes sont entrées en vigueur en République slovaque le 1^{er} janvier 2001. Le protocole additionnel à la Convention, concernant les autorités de contrôle et les flux transfrontières de données, a été ratifié en juillet 2002. La nouvelle loi n°428/2002 sur la protection des données personnelles, qui prévoit la création d'organismes de contrôle indépendants de la protection des

données personnelles, est entrée en vigueur le 1^{er} septembre 2002. Cette loi a ainsi donné lieu à la création d'un organisme gouvernemental autonome, l'Office de la protection des données personnelles.

La loi n°215/2002 relative à la signature électronique, adoptée par le Parlement en mars 2002, est entrée en vigueur le 1^{er} septembre 2002. Elle régit les relations concernant l'exécution et l'utilisation des signatures électroniques, les droits et responsabilités des personnes physiques et morales qui utilisent les signatures électroniques, la plausibilité et la protection des documents électroniques sur lesquels sont apposées des signatures électroniques.

RÉPUBLIQUE TCHÈQUE

Législation

Lois horizontales

La *Loi de protection des données à caractère personnel dans les systèmes d'information* est entrée en vigueur le 1^{er} juin 1992.¹⁵³ Elle concerne les données informatisées relatives aux personnes physiques et s'applique au secteur public et au secteur privé.

Cette loi suit de manière générale les principes des Lignes directrices de l'OCDE et comporte des dispositions spécifiques concernant les données sensibles. Elle prévoit des recours civils en cas de violation, qui peuvent être exercés par la voie judiciaire. Il n'existe pas pour le moment de commissaire à la protection des données en République tchèque.

Dans la perspective de l'adhésion de la République tchèque à l'Union européenne, le gouvernement a chargé l'*Office pour le système d'information de l'État* (OSIS) de rédiger une législation compatible avec la directive de l'Union européenne sur la protection des données¹⁵⁴. La nouvelle législation établira le statut d'un organisme de contrôle indépendant. Cette législation ne sera probablement pas adoptée par le Parlement avant le milieu de l'année 1999.

Autres lois comportant des dispositions de protection de la vie privée

L'*Office tchèque des télécommunications* prépare actuellement en coopération avec l'*Office pour le système d'information de l'État* un projet de loi qui transposera la directive 97/66/CE de l'Union européenne sur la protection de la vie privée dans le secteur des télécommunications. Un projet de loi sur les signatures numériques est également en préparation par le Bureau des systèmes d'information de l'État (OSIS), qui mettra en oeuvre les dispositions de la directive de l'Union européenne sur un cadre commun pour les signatures numériques.

ROYAUME-UNI

Législation

Lois horizontales

La loi de protection des données du Royaume-Uni (*Data Protection Act 1984*)¹⁵⁵ s'applique aux données informatisées à caractère personnel relatives aux personnes physiques dans le secteur public et le secteur privé. Elle donne aux personnes concernées un certain nombre de droits, notamment celui d'avoir accès aux données les concernant et de faire rectifier ou effacer les données erronées. Si une personne subit

un préjudice du fait de la perte, de la destruction non autorisée ou de la divulgation sans autorisation d'information la concernant, ou du fait de la diffusion de données erronées, celle-ci peut demander réparation devant les tribunaux.

La loi a créé une autorité de contrôle indépendante, appelée le *Data Protection Registrar*¹⁵⁶. Celui-ci a notamment pour fonction de créer et tenir un registre des personnes qui traitent des informations de caractère personnel. Le non-enregistrement d'une personne utilisant des données est passible de poursuites.

La loi définit huit principes de traitement loyal de l'information. Le Registrar enquête sur les plaintes concernant les violations de la loi et il peut émettre des mises en demeure contre des personnes enregistrées pour leur demander de prendre des mesures spécifiques de manière à se conformer à la loi. L'inobservation de ces mises en demeure constitue un délit pénal.

Le Registrar est également chargé de promouvoir la protection des données, notamment en encourageant l'élaboration de codes de pratiques sectoriels. Ces codes apportent une aide à l'interprétation de la loi. Le Registrar publie aussi des notes d'orientations, avec notamment une publication récente sur la « protection des données et l'Internet ».

Autres lois comportant des dispositions de protection de la vie privée

Un certain nombre de lois au Royaume-Uni ont des implications en matière de protection des données, notamment le *Financial Services Act 1986* (services financiers), le *Human Fertilisation and Embryology Act 1990*¹⁵⁷ (fécondation humaine et embryologie), le *Charities Act 1993*¹⁵⁸ (œuvres de bienfaisance) et le *Criminal Justice and Public Order Act 1994*¹⁵⁹ (justice pénale). Le gouvernement a aussi proposé une législation sur l'accès à l'information qui si elle était promulguée élargirait les droits d'accès à l'information et qui contient des dispositions d'exonération pour des motifs de protection de la vie privée ou autres.

La loi sur les droits de l'homme (*Human Rights Bill*)¹⁶⁰ de 1998 récemment adoptée transpose dans le droit national la Convention européenne des Droits de l'Homme¹⁶¹. Cette loi a été promulguée par la Reine le 9 novembre 1998, mais elle ne devrait pas entrer en vigueur avant 2000. Cette loi adopte notamment l'article 8 de la Convention, sur le droit au respect de la vie privée et familiale.

Mise en œuvre de la directive de l'Union européenne

La nouvelle loi de protection des données (*Data Protection Act 1998*)¹⁶² qui a été promulguée par la Reine le 16 juillet 1998 transpose la directive de l'Union européenne. Les détails de cette nouvelle loi seront pour une large part spécifiés dans une législation annexe. La nouvelle loi entrera en vigueur à la fin du mois de juin 1999, ou dès que le Gouvernement jugera cela possible.

Le législateur a élargi le champ d'application de la loi en vigueur en faisant entrer dans son champ d'application les données de caractère personnel contenues dans les fichiers manuels structurés. La définition du « traitement » et d'autres termes a été modifiée pour prendre en compte les définitions de la directive de l'UE. La loi de 1998 crée également de nouveaux droits pour les personnes concernées, notamment celui de refuser que les données les concernant soient utilisées pour des activités de vente directe ou de s'opposer à ce que des décisions importantes les concernant puissent être prises par des moyens automatiques, mais d'une manière plus générale elle prévoit un droit à indemnisation en cas de dommage découlant de toute violation de la nouvelle loi. Lorsque la nouvelle loi entrera en vigueur le *Data Protection Registrar* prendra la dénomination de *Data Protection Commissioner*.

Le *British Standards Institute* (Institut de normalisation) travaille avec le *Data Protection Registrar* à la réalisation d'un programme de mise en conformité en matière de protection des données dans la perspective de l'application de la directive de l'Union européenne.

Instruments d'autorégulation

Instruments concernant la protection de la vie privée en ligne

L'*Internet Service Providers Association (UK)*¹⁶³ (association des fournisseurs de service Internet) a élaboré un Code de conduite qui est facultatif pendant les 12 premiers mois puis rendu obligatoire pour tous ses membres. Ce Code sert de guide pour l'enregistrement auprès du *Data Protection Registrar*. Il engage aussi chaque membre de l'association à notifier aux utilisateurs les finalités pour lesquelles des informations à caractère personnel sont collectées et à leur donner la possibilité de s'opposer à l'utilisation de ces données.

Autres initiatives

Un certain nombre d'autres associations professionnelles ont publié des codes de conduite contenant des dispositions en matière de protection des données¹⁶⁴.

SUÈDE

Constitution

La Constitution suédoise (loi sur la liberté de la presse¹⁶⁵) garantit le droit des personnes à accéder aux documents et données détenus par les autorités publiques. De plus, la Constitution¹⁶⁶ stipule que les citoyens sont protégés, dans la mesure prévue en détail par la loi, contre toute violation de l'intégrité de leur personne du fait de l'enregistrement par des moyens électroniques d'information les concernant.

Législation

Lois horizontales

La loi sur les données personnelles¹⁶⁷ a été adoptée par le Parlement en avril 1998. Cette loi, qui est entrée en vigueur le 24 octobre 1998, transpose la directive de l'Union européenne en Suède. Elle offre un cadre légal pour tous les traitements de données à caractère personnel, et elle est appuyée par une réglementation du gouvernement¹⁶⁸ et l'Inspection des données (*Datainspektionen*). Toutefois, les dispositions de la loi ne s'appliquent pas, notamment, si elles sont contraires aux dispositions relatives à la liberté de la presse et à la liberté d'expression contenues dans la loi sur la liberté de la presse et la loi fondamentale sur la liberté d'expression.¹⁶⁹

La loi confère à l'Inspection des données une mission de surveillance et de conseil.

Les pénalités en cas d'infraction à la loi comprennent principalement des dommages-intérêts en faveur de la personne qui a subi un préjudice.

Autres lois comportant des dispositions de protection de la vie privée

La Loi sur les informations en matière de crédit, la Loi sur le recouvrement des créances et la Loi sur les statistiques officielles sont d'autres lois suédoises comportant des dispositions de protection de la vie privée.

Instruments d'autorégulation

L'Association suédoise du marketing direct est engagée dans des activités en matière d'autorégulation.

SUISSE

Législation

Lois fédérales

La *Loi fédérale sur la protection des données* (LPD) (1992)¹⁷⁰ s'applique aux fichiers informatisés ou manuels concernant les personnes physiques et les personnes morales dans le secteur public fédéral et dans le secteur privé. Le *Préposé fédéral à la protection des données*¹⁷¹ (nommé par le *Conseil fédéral*) supervise l'application de la loi par les autorités fédérales et sert de médiateur pour le traitement des données à caractère personnel dans le secteur privé. Tous les fichiers fédéraux doivent être enregistrés auprès du Préposé, mais les organisations privées ne sont tenues de faire enregistrer leurs fichiers que dans des cas limités¹⁷². Le Préposé a aussi pour mission d'assister les organismes de protection de la vie privée fédéraux et cantonaux et d'examiner dans quelle mesure les régimes de protection des données étrangers assurent une protection comparable. Le Préposé peut aussi conduire des enquêtes (de sa propre initiative ou à la demande d'un tiers) et émettre des recommandations. Le Préposé a une fonction principalement consultative dans le secteur privé. Il peut aussi être une instance d'arbitrage et de recours¹⁷³.

La LPD repose sur les principes de base des Lignes directrices de l'OCDE. Les données sensibles reçoivent une protection spéciale. La LPD interdit les transferts transfrontières de données si une protection adéquate des données n'est pas garantie, et une déclaration préalable au Préposé est requise pour ces transferts dans certains cas.

Les personnes concernées peuvent recourir aux voies de droit habituelles du Code civil suisse¹⁷⁴, comme les injonctions et les ordonnances d'indemnisation, pour les infractions à la LPD. Ces infractions sont aussi punissables par des peines d'amende ou d'emprisonnement.

Autres lois fédérales comportant des dispositions de protection de la vie privée

Un certain nombre de lois suisses contiennent des dispositions de protection de la vie privée, notamment : la loi sur les télécommunications, la législation des contrats de travail, la loi sur la statistique fédérale et le *Code pénal suisse*. Il existe aussi une *Ordonnance concernant les autorisations de lever le secret professionnel en matière de recherche médicale* (1993).

Lois des Cantons

Les activités des autorités cantonales sont régies par le droit cantonal. La plupart des Cantons suisses ont établi des lois de protection des données qui s'appliquent à ces organismes. Les règles applicables sont en général semblables à celles du niveau fédéral et comprennent l'établissement d'organismes de protection des données.

Instruments d'autorégulation

Instruments concernant la protection de la vie privée dans les communications en ligne

Un groupe de travail de l'*Office fédéral de la justice* a formulé des recommandations à l'usage des fournisseurs de service Internet (le *Code suisse*). Ce Code contient des recommandations sur des questions juridiques comme la responsabilité des fournisseurs de services et la divulgation de données à des tiers.

Autres initiatives

Des codes de pratique sectoriels apportent un complément d'orientation dans des domaines spécifiques comme la profession médicale, la vente directe ou les études de marché. Il existe des obligations de secret bien connues dans les domaines de la banque, de l'assurance et des retraites.

TURQUIE

Législation

La Turquie a un projet de loi sur la protection des données applicable aux entités qui traitent des données aussi bien dans le secteur public que dans le secteur privé. Ce projet de loi n'a pas encore été voté par le Parlement turc. Il intègre les principes de base des Lignes directrices de l'OCDE et de la Convention 108 et il établit une *Autorité de la protection des données* autonome. L'Autorité doit superviser l'application de la loi.

Aux termes de ce projet de loi, une personne aura le droit d'être informée chaque fois que des données seront collectées, d'accéder aux données la concernant, de les rectifier lorsqu'elles sont erronées et de s'opposer à certains types de traitement.

Par ailleurs, les travaux sur le commerce électronique ont débuté en Turquie au mois de février 1998, suite à une décision du Conseil supérieur de la science et de la technologie (*Science and Technology High Board -- STBH*). Trois groupes de travail relevant de la Commission de coordination sur le commerce électronique ont été chargés des études. Un premier rapport établi par ces groupes a été soumis au Conseil supérieur en juin 1998. Ce rapport analyse les obstacles qui entravent le commerce électronique en Turquie et il propose des recommandations, notamment l'élaboration de procédures d'authentification et de certification, afin d'éliminer de façon satisfaisante ces obstacles. La phase suivante consistera à établir un plan d'action devant être soumis au Conseil supérieur. Cette étude examinera notamment la question des ressources humaines, des échéances et des organisations à assigner pour améliorer l'infrastructure juridique, technique et financière dont le commerce électronique a besoin pour se développer.

II. Mécanismes visant à mettre en œuvre et faire respecter les principes de protection de la vie privée sur les réseaux mondiaux

Il existe diverses pratiques, techniques ou technologies, actuellement employées ou en cours d'élaboration, destinées à mettre en œuvre et faire respecter les principes de protection de la vie privée dans des environnements de réseaux. Ces différents mécanismes sont liés les uns aux autres ; beaucoup reposent sur des progrès technologiques récents et certains gommant les distinctions traditionnelles entre établissement des principes gouvernant la protection de la vie privée, mise en œuvre et exécution. Certains permettent aux utilisateurs de prendre en charge la protection de leurs données personnelles et de leur vie privée (par exemple, en empêchant le transfert et la collecte des informations d'en-tête et des données sur la « succession des clics »), d'autres sont mis en œuvre par les responsables de fichier (par exemple, en apposant un label numérique concernant les pratiques du site Web en matière de protection de la vie privée) et d'autres peuvent être facilités par les gouvernements et/ou les organisations du secteur privé (par exemple, avec la création de clauses types pour les contrats régissant les flux transfrontières de données).

Dans cette partie de l'Inventaire, les divers mécanismes de protection de la vie privée sur les réseaux mondiaux sont répartis entre différentes catégories, suivant qu'ils ont pour but :

- De réduire au minimum la communication et la collecte de données à caractère personnel.
- D'informer les utilisateurs sur les politiques de protection de la vie privée en ligne.
- D'offrir aux utilisateurs un choix concernant la communication et l'utilisation des données à caractère personnel.
- De donner accès aux données personnelles.
- De protéger la vie privée au moyen de contrats régissant les flux transfrontières de données.
- De faire respecter les principes de la protection de la vie privée ; ou
- D'éduquer les utilisateurs et le secteur privé.

A. Réduire au minimum la communication et la collecte des données à caractère personnel

Les utilisateurs des réseaux mondiaux peuvent agir dans un anonymat relatif en réduisant la quantité de données à caractère personnel qu'ils révèlent et/ou qu'ils permettent de collecter¹⁷⁵. C'est un moyen de protection de la vie privée important. Pour aider à préserver l'anonymat en ligne, il existe des mécanismes qui : (i) permettent aux utilisateurs de restreindre la communication et la collecte automatiques de données retraçant la navigation sur le Web et (ii) réduisent le besoin de révéler volontairement des données à caractère personnel.

1. Restreindre ou éliminer la communication et la collecte automatiques de données personnelles

Comme cela a été indiqué dans l'introduction générale, des informations d'en-tête et des données sur la succession des clics peuvent être communiquées à chaque fois que l'on visite un site Web et des « cookies » sont souvent employés pour faciliter la collecte de ces données. En général, un utilisateur peut renforcer son anonymat en limitant la création de « cookies », ou en empêchant le transfert, et la collecte, de données générées automatiquement (informations d'en-tête, en-têtes de courrier électronique et données sur la succession des clics) à partir de son ordinateur. Ces deux techniques permettent aux utilisateurs de prendre eux-mêmes en charge la protection de leur vie privée.

a) Gestion des « cookies »

Dans la mesure où les « cookies » peuvent être utilisés pour associer un numéro de code à un utilisateur donné, l'un des moyens de préserver l'anonymat quand on utilise le Web consiste à permettre aux utilisateurs de restreindre ou d'empêcher la création de « cookies ». Ainsi, par exemple :

- Les versions les plus récentes de *Microsoft Explorer* et de *Netscape Communicator* permettent aux utilisateurs de définir leurs préférences afin d'être avertis quand un serveur essaie de placer un cookie et d'avoir la possibilité de refuser sa création.
- Des applications logicielles ont été conçues qui suppriment automatiquement les « cookies » non autorisés (certaines de ces applications peuvent aussi contrôler les informations d'en-tête qui sont transférées du client vers le site Web). *Internet Junkbuster Proxy*¹⁷⁶ et *Cookie Crusher*¹⁷⁷ en sont des exemples.

Ces technologies exigent un degré appréciable de compétence de la part de l'utilisateur et elles n'empêchent pas en général le serveur d'obtenir du logiciel de navigation de l'utilisateur les informations d'en-tête de base. Toutefois, de nouvelles évolutions de la technologie pourraient rendre leur utilisation plus rationnelle et plus efficace.

b) Empêcher le transfert et la collecte des données générées automatiquement

Il existe des mécanismes permettant d'empêcher le transfert et/ou la collecte de données générées automatiquement, comme les en-têtes de courrier électronique, les informations d'en-tête et les données sur la succession des clics.

Les « services de courrier anonyme » permettent d'envoyer des messages de courrier électronique sans que soit révélée l'identité de l'expéditeur. Certains, comme *Hotmail*¹⁷⁸ ou le *Freedom Remailer*, géré par la *Global Internet Liberty Campaign*¹⁷⁹, fonctionnent au moyen de pages Web où l'on crée et envoie un message électronique sans aucune information identifiant l'expéditeur. D'autres services sont conçus pour recevoir un message électronique d'un premier utilisateur, rétablir la destination du message et l'envoyer au destinataire. Dans ce processus, les informations d'en-tête qui auraient identifié l'expéditeur sont supprimées. Les services de *Replay* ou *Nymserver* en sont des exemples. Ces services de courrier anonyme offrent différents degrés de protection en vue d'empêcher que l'interception des messages passant par ce réexpéditeur permette d'identifier l'expéditeur et aussi d'empêcher que l'on puisse faire des recoupements basés, par exemple, sur la longueur des messages et les informations temporelles (Goldberg *et al.*, 1997). Beaucoup de services de courrier anonymes ont été obligés de fermer en raison du fait que des abus ont été commis, tel l'envoi de messages malveillants ou le publipostage.

On peut utiliser un « intermédiaire d'anonymat » pour empêcher un site Web de collecter automatiquement les informations d'en-tête concernant les utilisateurs¹⁸⁰, d'associer les données de succession des clics à un utilisateur particulier ou de placer des « cookies » dans l'ordinateur des utilisateurs. L'intermédiaire est un serveur Web qui opère entre l'utilisateur et le reste du Web. Quand l'utilisateur souhaite voir une page Web, il demande cette page à l'intermédiaire. L'intermédiaire obtient la page et la remet à son tour à l'utilisateur. Comme l'utilisateur n'est jamais connecté directement au site qu'il visite, aucune information d'en-tête concernant l'utilisateur n'est transmise et le site Web n'a pas non plus la possibilité de placer un cookie sur l'ordinateur de l'utilisateur. L'*Anonymizer*¹⁸¹ est un exemple de ce genre de service.

La nécessité que les intermédiaires d'anonymat suivent de bonnes pratiques en matière de protection des données et les risques d'abus de l'anonymat¹⁸² sont deux questions que l'utilisation de ces services a soulevées.

2. Réduire ou éliminer la nécessité de communiquer volontairement ses données

L'une des raisons pour lesquelles des données à caractère personnel sont demandées sur les réseaux mondiaux tient au besoin d'établir la preuve qu'un utilisateur peut être admis à faire une certaine transaction ou que les informations relatives au paiement sont authentiques. Des mécanismes sont actuellement élaborés qui, s'ils sont adoptés par les utilisateurs et les entreprises en ligne, permettront la vérification de ces éléments sans requérir la communication d'informations à caractère personnel.

a) Systèmes de paiement anonyme

Certains mécanismes de paiement entraînent la communication d'un plus grand nombre de données que d'autres. Dans le monde hors ligne, le moyen de paiement le plus anonyme est le paiement en espèces. La valeur des espèces étant inhérente et irréfutable, ceux qui les encaissent n'ont pas besoin de garanties d'authenticité supplémentaires. En comparaison, d'autres mécanismes de paiement comme les cartes de crédit nécessitent souvent la communication de données à caractère personnel (comme le nom et l'adresse de facturation du payeur) afin d'authentifier le paiement. La faculté d'effectuer des transactions de type espèces dans le monde en ligne renforce l'anonymat de l'utilisateur et restreint les possibilités de faire le lien entre, d'un côté, les informations d'en-tête et les données de succession de clics et, de l'autre, une identité du monde réel.

Un certain nombre d'entreprises mettent au point des mécanismes de paiement de type espèces à utiliser sur les réseaux mondiaux¹⁸³. *Mondex*¹⁸⁴ est un exemple. En l'espèce, l'argent est placé dans une « carte à puce »¹⁸⁵ et les transactions s'effectuent directement entre les parties sans être déclarées à un ordinateur central. Pour des raisons de sécurité et des raisons pratiques, des relevés de contrôle sur période mobile sont enregistrés sur chaque carte et chez les commerçants. On peut révéler le contenu de ces relevés pour résoudre les litiges, corriger les transactions défectueuses ou sur ordre des autorités légales. Toutefois, dans les transactions normales, la vie privée de l'utilisateur est protégée parce que le commerçant n'a pas accès aux informations de la banque qui associent le nom d'une personne au numéro de référence de sa carte Mondex.

Comme les systèmes de paiement dans le monde hors ligne, les mécanismes de paiement électronique ont aussi leurs limites. Premièrement, il s'y attache des externalités de réseau et ils ne sont viables que si une masse critique de commerçants les accepte. Deuxièmement, la divulgation d'informations à caractère personnel reste possible si, par exemple, l'acheteur donne son nom et son adresse pour la livraison du produit ou si le commerçant est en mesure de collecter des informations révélant l'identité, telles que l'adresse de courrier électronique de l'utilisateur. Enfin, certains commentateurs craignent que les mécanismes de paiement anonyme ne facilitent le blanchiment de fonds, l'escroquerie et la fraude fiscale. Toutefois, ces systèmes de paiement sont un outil important pour protéger la vie privée, notamment lorsqu'ils sont couplés à d'autres technologies et à des politiques en matière de vie privée.

b) Certificats numériques

Un autre moyen potentiel de faciliter les transactions anonymes dans une relation sans face à face sur les réseaux mondiaux consiste à utiliser des « certificats numériques » reposant sur des techniques de cryptographie à clé publique pour attester certains attributs individuels sans révéler le nom de la personne considérée ou d'autres informations d'identification (Froomkin, 1996).

Les certificats numériques délivrés par une source de confiance, telle qu'une « autorité de certification », peuvent assurer une vérification indépendante d'informations telles que l'identité ou les éléments d'une transaction. Dans un contexte tendant à réduire au minimum la communication de données à caractère personnel et à préserver l'anonymat sur les réseaux mondiaux, peuvent être délivrés des certificats numériques qui attestent certains attributs individuels comme l'âge, le lieu de résidence, la nationalité, le droit d'utiliser un service ou l'appartenance à une organisation, sans révéler l'identité de la personne qui effectue la transaction. Ces certificats peuvent réduire ou éliminer la nécessité de communiquer des données personnelles dès lors que le point important n'est pas de savoir qui est la personne concernée mais de vérifier si elle possède ou non une certaine caractéristique. Par exemple, un commerçant qui vend dans l'environnement électronique des produits interdits aux mineurs peut se contenter d'un certificat numérique qui déclare qu'un certain consommateur a l'âge qui convient, sans avoir besoin de connaître son identité.

L'utilisation de certificats numériques pour attester des attributs individuels soulève un certain nombre de questions qu'il faut sans doute examiner de plus près, comme le problème des attributs qui changent au cours du temps, la fraude ou la nécessité que les autorités de certification, qui peuvent détenir de grandes quantités de données à caractère personnel, suivent de bonnes pratiques de protection de la vie privée.

c) Profils anonymes

Une autre raison pour laquelle les sites Web collectent des données sur les utilisateurs et leurs habitudes de navigation est la création de profils qui peuvent faciliter le ciblage du contenu publicitaire, rédactionnel ou commercial en fonction de chaque visiteur. Cependant, cela peut se faire au moyen de « profils anonymes » qui révèlent les informations souhaitées sur les habitudes de navigation sans contenir d'information susceptible d'identifier la personne. Par exemple, *Engage Technologies*¹⁸⁶ a créé une base de données de 16 millions de profils d'utilisateurs du Web au moyen de « cookies » servant à attribuer un identifiant numérique propre à chaque personne qui visite un site Web équipé pour ce dispositif. *DoubleClick*¹⁸⁷ et *Clickstream*¹⁸⁸ sont deux autres compagnies qui exploitent des systèmes similaires.

Ces systèmes ont suscité un certain nombre de préoccupations concernant la protection de la vie privée : si ces profils sont, en un sens, anonymes, il n'en demeure pas moins qu'ils donnent lieu à la collecte d'une grande quantité de données qui peuvent faire l'objet d'un commerce, avoir des répercussions sur les sessions de navigation futures et, éventuellement, être associées ultérieurement à l'identité réelle de l'utilisateur.¹⁸⁹

B. Informer les utilisateurs sur les politiques de protection de la vie privée en ligne

Il y a un équilibre à trouver entre les avantages que procure, d'une part, le recours à l'anonymat et, d'autre part, la révélation d'informations à caractère personnel pour participer pleinement au large éventail d'interactions, de relations et de communications qui s'offre sur les réseaux internationaux. En outre,

beaucoup d'utilisateurs n'ont pas les connaissances nécessaires, ou ne sont pas préparés à faire l'effort nécessaire, pour maintenir la confidentialité des données les concernant.

Le pourcentage des sites Web qui contiennent actuellement des déclarations sur leurs pratiques en matière de protection de la vie privée et des données personnelles continue de croître¹⁹⁰. Diverses entités privées (comme *TRUSTe*¹⁹¹ et *BBBOnline*¹⁹²) et associations professionnelles (comme l'*Online Privacy Alliance*¹⁹³ et l'*American Electronics Association*¹⁹⁴) cherchent à promouvoir l'adoption de pratiques appropriées pour l'information des utilisateurs et de normes communes pour la protection de la vie privée. Par exemple, dans le dispositif de licences de TRUSTe, les sites participants doivent, au minimum, déclarer leur politique en indiquant quelles informations ils collectent, ce qui est fait de ces informations, avec qui ils les partagent et les possibilités de refus offertes à l'utilisateur¹⁹⁵. Un facteur important pour que les utilisateurs soient convaincus que les sites Web appliquent effectivement les politiques de protection de la vie privée qu'ils annoncent réside dans les mécanismes employés pour assurer le respect de ces politiques et pour apporter réparation si elles sont enfreintes. Ces mécanismes sont examinés plus loin.

Il existe différentes façons pour un site Web d'informer ses visiteurs sur les données à caractère personnel qu'il collecte (le cas échéant) et sur l'utilisation qui en sera faite : (i) l'affichage de sa politique de protection de la vie privée ; (ii) les clauses des accords en ligne ; (iii) les étiquettes numériques.

1. *L'affichage des politiques de protection de la vie privée*

Pour une organisation menant des activités en ligne, le moyen le plus simple de déclarer sa politique de protection de la vie privée consiste à le faire sur une page spécifique de son site Web. Les politiques de protection de la vie privée des sites Web devraient prendre en compte les Lignes directrices de l'OCDE et pourraient contenir les informations suivantes¹⁹⁶ : identité de l'organisation qui collecte les données et moyens par lesquels on peut entrer en contact avec elle ; personne responsable, dans l'organisation, du respect de la politique de protection de la vie privée ; nature des informations collectées et moyens de collecte ; nature de l'utilisation des données collectées ; choix offerts à l'utilisateur concernant la collecte, l'utilisation et la distribution des données ; mesures de sécurité employées ; façon dont les personnes concernées peuvent accéder à leurs informations et les faire corriger ; recours en cas de violation de la politique ; législation de protection de la vie privée ou codes de conduite éventuellement applicables ; procédures d'audit ou de certification éventuellement appliquées ; technologies utilisées pour renforcer la protection de la vie privée. On trouve aussi quelquefois les politiques de protection de la vie privée dans les sections « Foire aux questions » (FAQ) ou « Aide » des sites Web.

Pour compléter les informations présentées dans ce type de déclaration, certains sites Web proposent des liens hypertextes pour diriger les visiteurs vers des informations sur les questions relatives à la protection de la vie privée, les organisations de protection de la vie privée et certains aspects techniques, tels les « cookies ». On peut aussi faciliter l'accès à une politique de protection de la vie privée en offrant des liens hypertextes à partir de lieux appropriés, comme la page d'accueil du site et toutes les pages où l'on demande des données à caractère personnel, et en incluant « protection de la vie privée » dans l'index des termes clés si le site a un moteur de recherche interne. Le développement « d'icônes de protection de la vie privée » reconnues, avec des liens hypertextes vers les politiques de protection de la vie privée des sites Web, peut aussi accroître la facilité d'accès à ces politiques. Ces icônes peuvent avoir des fonctions additionnelles, comme de signaler que la politique de protection de la vie privée et les pratiques en matière d'information du site considéré satisfont aux exigences d'un tiers certificateur.

2. *Clauses*

Un site Web peut inclure sa politique de protection de la vie privée dans les modalités et conditions qui sont applicables entre le site et ses visiteurs. Par exemple, quand un site Web demande à l'utilisateur d'accepter une inscription d'une forme ou d'une autre pour pouvoir accéder aux parties non publiques du site, une clause de protection de la vie privée y est souvent incluse¹⁹⁷. Comme les autres moyens de notification, les clauses de protection de la vie privée incluses dans les modalités et conditions en ligne sont très variables quant à leur étendue et au degré de protection de la vie privée qu'elles offrent à l'utilisateur.

3. *Étiquettes numériques*

La « Labellisation numérique » des pratiques de protection de la vie privée peut constituer un moyen de notification différent ou complémentaire. L'idée de base est d'utiliser un « vocabulaire » uniforme, mis au point par une organisation ou un groupe particulier menant des activités en ligne, pour décrire les pratiques adoptées par chaque site à l'égard des informations. Cette description revêt la forme d'un label inclus dans l'en-tête d'une page Web et lisible par le logiciel de navigation de l'utilisateur.

Le projet *Platform for Privacy Preferences* (P3P)¹⁹⁸ est fondé sur cette approche. P3P, en cours d'élaboration par le World Wide Web Consortium (W3C), repose sur une autre structure du Consortium qui permet le label des sites Web et est appelée *Platform for Internet Content Selection* (PICS)¹⁹⁹. P3P vise à permettre aux sites Web d'exprimer simplement leurs pratiques de protection de la vie privée concernant la collecte et l'utilisation des données à caractère personnel et de donner aux utilisateurs la possibilité de spécifier leurs propres préférences²⁰⁰. Le vocabulaire de protection de la vie privée en cours d'élaboration contient actuellement une liste de catégories de données et de pratiques à l'égard des données concernant, par exemple, les finalités pour lesquelles les données sont utilisées ou communiquées, la possibilité pour la personne concernée d'accéder aux données enregistrées et de les corriger, ainsi que l'identité de la personne à qui adresser les réclamations²⁰¹.

P3P est le médiateur de l'interaction entre les options de protection de la vie privée du site et celles de l'utilisateur. Pour les sites dont les pratiques correspondent à l'ensemble de préférences de l'utilisateur, l'accès s'effectue de manière « transparente ». Dans d'autres cas, l'utilisateur reçoit une déclaration des pratiques du site et peut accepter ces modalités ou se voir offrir d'autres modalités, ou bien quitter le site.

C. Offrir aux utilisateurs un choix concernant la communication et l'utilisation des données à caractère personnel

Il peut être tiré parti de l'interactivité des réseaux mondiaux pour offrir aux utilisateurs un choix quant aux informations qu'ils sont disposés à révéler et à l'usage qui en sera fait.

1. Rubriques optionnelles et choix de cases à cliquer

Certains sites Web offrent un choix en collectant les données au moyen de formulaires en ligne qui distinguent parmi les rubriques à remplir celles qui sont obligatoires ou optionnelles, et qui présentent des « cases à cliquer » offrant aux visiteurs des options quant à l'usage qui peut être fait des informations fournies. Par exemple, les données obligatoires peuvent comprendre les données d'identification et de paiement nécessaires à une transaction entre les parties, tandis que les données optionnelles peuvent être l'âge, le sexe, la profession et diverses préférences personnelles de l'utilisateur. Concernant les options

relatives à l'utilisation des données, les visiteurs peuvent avoir des cases à cliquer indiquant s'ils acceptent ou non que leurs données servent à des fins de marketing et/ou soient communiquées à des tiers.

Des compagnies dont l'activité consiste à fournir des profils personnels à d'autres sites Web ont élaboré une approche similaire permettant à chaque personne de garder la maîtrise de la communication des données qui la concerne. *Firefly* est un exemple de ce genre de système. Un utilisateur de *Firefly* crée un « passeport » qui contient les informations qu'il accepte de divulguer sur le Web. Ce passeport, qui est en fait un profil personnel de ce qu'il accepte et de ce qu'il refuse, est alors instantanément présenté aux sites membres que l'utilisateur visite. *MatchLogic*²⁰² emploie un système similaire. Il attribue à chaque utilisateur qui visite un de ses sites un numéro aléatoire propre à cet utilisateur, ce au moyen d'un cookie²⁰³. Ce numéro sert à retracer la succession des clics concernant, par exemple, les types de publicités que regarde l'utilisateur.

2. *Négociation en ligne d'options de protection de la vie privée au moyen des labels numériques*

Le label numérique et le filtrage automatique, examinés ci-dessus, peuvent aussi servir à présenter à l'utilisateur de nouvelles options quand les pratiques standard d'un site Web en matière de protection de la vie privée ne correspondent pas aux préférences que l'utilisateur a fixées dans son logiciel de navigation. Cela représente une forme simple de négociation en ligne.

3. *Faculté de refus*

Maîtriser l'utilisation des données à caractère personnel après la collecte

Pour permettre aux utilisateurs de faire savoir qu'ils ont changé d'avis sur l'usage qui peut être fait de leurs données, certains sites Web acceptent de recevoir leurs décisions par courrier électronique, courrier ordinaire ou téléphone.

Éviter la réception de messages électroniques publicitaires importuns

Il existe aussi diverses technologies ou pratiques pour éviter de recevoir des publicités importunes par le courrier électronique. Un moyen consiste pour l'utilisateur à adopter des outils de filtrage pour bloquer les messages électroniques provenant de sociétés de publipostage électronique connues. Une autre pratique consiste à donner au destinataire d'un publipostage électronique non sollicité la possibilité de répondre à l'expéditeur pour demander qu'on ne lui envoie plus de messages à cette adresse. Plus largement, il peut être développé une « liste d'exclusion » ou « liste orange »²⁰⁴ pour le courrier électronique (*E-mail Preference Service* (e-MPS) ou *E-mail Robinson List*). Ce type de liste permet aux consommateurs qui ne souhaitent pas recevoir de sollicitations commerciales par le courrier électronique d'inscrire leur adresse dans un registre commun que les entreprises participantes utilisent pour rayer ces personnes de leurs propres listes²⁰⁵. La *Direct Marketing Association* des Etats-Unis élabore actuellement un système de ce genre et a l'intention d'en rendre l'utilisation obligatoire pour ses membres à partir de juillet 1999 (DMA, 1998)²⁰⁶. Une autre proposition, provenant du *Data Protection Registrar* britannique, est d'utiliser dans les adresses électroniques un caractère universellement reconnu pour indiquer que l'utilisateur ne veut recevoir aucune sollicitation commerciale.

Opposition à des profils anonymes

Il existe actuellement différentes approches concernant les données qui ont été collectées automatiquement à partir des informations d'en-tête et des successions de clics. Dans les systèmes de profils anonymes exploités par *Engage Technologies* et *MatchLogic*, les données de succession de clics collectées automatiquement ne sont pas considérées comme des « données à caractère personnel » sur lesquelles l'utilisateur a le droit d'exercer un contrôle. En revanche, le système *DoubleClick*, qui utilise aussi des « cookies » pour attribuer des numéros d'identification propres à chaque utilisateur et collecter des données de succession de clics, offre aux utilisateurs une option de refus. Si l'utilisateur la choisit, le numéro d'identification est effacé et les données de succession de clics ne sont plus enregistrées²⁰⁷.

D. Donner accès aux données personnelles

On peut offrir à une personne l'accès aux données qui la concernent au moyen de mécanismes classiques hors ligne (comme le courrier postal ou le téléphone) ou par des procédures en ligne interactives où la demande et la réponse s'exécutent en temps réel pendant la connexion entre le site Web et la personne en question.

E. Protéger la vie privée au moyen de contrats régissant les flux transfrontières de données

Les contrats régissant les flux transfrontières de données constituent un moyen important pour mettre en œuvre les Principes de protection de la vie privée dans le contexte d'un transfert de données à caractère personnel entre un responsable de fichier situé dans un pays et un autre responsable de fichier situé dans un pays différent. Ces contrats offrent un moyen de protéger les données à caractère personnel transférées entre des zones de compétence qui peuvent avoir des régimes juridiques différents, à l'égard de la protection de la vie privée.

Beaucoup de textes internationaux prévoient un traitement spécial pour les flux transfrontières de données. Par exemple, la Partie Trois des Lignes directrices de l'OCDE stipule qu'un pays membre peut, pour certaines catégories de données à caractère personnel pour lesquelles sa législation interne prévoit des dispositions spécifiques, imposer des restrictions aux flux à destination de pays membres qui n'ont pas de protection « équivalente ». L'article 12 de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 ») contient une disposition similaire. Cette question est particulièrement à l'ordre du jour en raison de l'article 25(1) de la directive de l'Union européenne sur la protection des données qui stipule que les transferts de données d'un pays membre vers un pays tiers ne peuvent avoir lieu que si ce dernier assure « un niveau de protection adéquat ». Les contrats régissant les flux transfrontières de données peuvent établir une passerelle entre des systèmes de protection de la vie privée différents si l'importateur des données n'est pas considéré comme offrant une protection adéquate²⁰⁸.

Le contrat-type du Conseil de l'Europe, de 1992, et le Guide relatif à l'élaboration de clauses contractuelles régissant la protection des données lors de communications de données à caractère personnel à des tiers non soumis à un niveau de protection des données adéquat (2002)

Le *Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données* (« Contrat-type ») du Conseil de l'Europe est le résultat d'une étude conjointe du Conseil de l'Europe, de la Commission des communautés européennes et de la Chambre de commerce internationale (CCI). Ce contrat est un ensemble de clauses types conçues pour assurer une « protection équivalente » dans le contexte des flux transfrontières de données basée sur les garanties de la Convention 108. Outre le fait qu'il peut répondre à la clause de protection équivalente dans les Lignes directrices de l'OCDE, le Contrat-type du Conseil de l'Europe peut aussi constituer une référence utile pour déterminer ce qui peut représenter une « protection adéquate » selon la directive de l'Union européenne.

Aux termes du Contrat-type, la partie qui envoie les données garantit qu'elles ont été obtenues et traitées conformément à la législation interne régissant la protection de la vie privée dans le pays où elle opère. En particulier il est fait référence aux éléments suivants : collecte loyale et licite des données, finalités pour lesquelles les données ont été enregistrées, adéquation et pertinence des données, exactitude des données et durée de conservation autorisée.

La partie qui reçoit les données s'engage à respecter les mêmes principes que ceux qui s'appliquent à l'expéditeur des données dans le pays de ce dernier. Pour compléter cet engagement, le destinataire des données accepte aussi de n'utiliser les données que pour les finalités énoncées dans le contrat, de protéger les données sensibles de la manière exigée par le droit interne de l'expéditeur, de ne pas communiquer les données à un tiers sauf si c'est expressément autorisé dans le contrat et de rectifier, effacer ou mettre à jour les données sur instruction de l'expéditeur des données.

Les autres clauses traitent de la responsabilité du destinataire en cas d'usage abusif des données, des droits des personnes concernées²⁰⁹, du règlement des conflits et de la résiliation du contrat. Les parties sont libres de convenir du droit applicable.

En 2002, le Conseil de l'Europe a adopté un Guide relatif à l'élaboration des clauses contractuelles régissant la protection des données lors de communications de données à caractère personnel à des tiers non soumis à un niveau de protection des données adéquat, qui complète et affine le contrat-type de 1992. Ce guide aide les parties à rédiger des clauses contractuelles conformes aux normes de protection découlant de la Convention n° 108, informe les maîtres de fichiers et les personnes concernées par les flux transfrontaliers de ce à quoi ils doivent prêter attention et aide les personnes concernées dans l'exercice de leurs droits en matière de protection des données. C'est pourquoi ce guide ne remplace pas les clauses contractuelles contenues dans le contrat-type de 1992 ; les deux documents doivent être lus l'un par rapport à l'autre.

Le Contrat-type révisé de la CCI

La Chambre de commerce internationale a révisé les clauses du contrat-type de 1992 à la lumière de la « protection adéquate » exigée par la directive de l'Union européenne pour les échanges de données vers les pays tiers²¹⁰. Cette révision prend en compte les commentaires du groupe de travail de la Commission européenne établi conformément à l'article 29 de la directive²¹¹.

Un exemple d'accord : Chemins de fer allemands (Deutsche Bahn AG) - Citibank

En 1994, les Chemins de fer allemands (Deutsche Bahn AG) ont établi avec la filiale allemande de Citibank un arrangement pour produire des cartes RailwayCards (offrant des réductions de prix aux voyageurs qui prennent souvent le train) fonctionnant aussi comme des cartes VISA (Dix, 1996). Comme les cartes étaient produites par une filiale de Citibank aux Etats-Unis, cet arrangement donnait lieu à d'importants flux transfrontières de données. En réponse aux préoccupations exprimées en Allemagne au sujet de la protection des données, un Accord sur la protection interterritoriale des données fut signé pour assurer aux citoyens allemands le même degré de protection de la vie privée que si les cartes avaient été produites en Allemagne. En particulier, ce contrat prévoyait l'application du droit allemand, limitait le transfert des données à des tiers, permettait des audits sur place dans les filiales de Citibank aux Etats-Unis par les autorités allemandes de protection des données et stipulait que les Chemins de fer allemands et la filiale allemande de Citibank étaient responsables à l'égard des personnes concernées en Allemagne en cas de violation de cet accord par leurs partenaires américains.

F. *Faire respecter les principes de protection de la vie privée*

Les mécanismes utilisés pour faire respecter les principes de protection de la vie privée varient d'un pays à l'autre. En particulier, l'équilibre établi entre le recours à la législation et l'autorégulation peut être différent. En outre, les préoccupations que suscitent les réseaux mondiaux en matière de protection de la vie privée ont conduit à la mise au point de nouvelles solutions technologiques, institutionnelles et contractuelles qui commencent à recueillir l'adhésion dans différentes parties du monde. Par exemple, la certification par des tiers de confiance qu'un site Web respecte la politique de protection de la vie privée qu'il affiche, apparaît comme un nouveau mécanisme développé par le secteur privé pour faire respecter les principes de protection de la vie privée.

Quel que soit le régime considéré, la mise à exécution des principes revêt deux aspects. Le premier concerne les mécanismes conçus pour s'assurer, *a priori*, que les principes seront appliqués dans la pratique. Le deuxième aspect concerne ce qui se passe en cas d'infraction aux principes de protection de la vie privée. En particulier, auprès de qui une personne concernée peut-elle porter plainte, de quels recours disposent les parties victimes d'un préjudice et comment les responsables de fichier peuvent-ils être contraints à obéir aux principes applicables ? Cette distinction entre examen de conformité *a priori* et procédures de « résolution des plaintes » *a posteriori* est adoptée dans les développements qui suivent, consacrés aux mécanismes dont on dispose pour faire respecter les principes de la protection de la vie privée²¹².

1. *Assurer la conformité aux normes de protection de la vie privée*

Il existe beaucoup de moyens pour veiller *a priori* au respect des principes de protection de la vie privée quelle que soit l'origine de ces principes (législation, codes de conduite ou accords entre entreprises et consommateurs). Dans l'exposé qui suit, on distingue quatre types de moyens pour assurer la conformité : désignation d'un responsable interne de la protection des données ; certification de conformité par une tierce partie ; adhésion à des associations professionnelles qui imposent des normes de protection de la vie privée ; et contrôles par une autorité centrale de surveillance.

a) Responsables internes de la protection des données

Les législations de protection de la vie privée et les codes d'autorégulation peuvent exiger la nomination, par les responsables de fichier, d'un responsable interne chargé de la protection des données²¹³ ou la désignation à l'intérieur d'une organisation d'un responsable précisément chargé de veiller à ce que l'organisation se conforme aux pratiques applicables en matière de protection de la vie privée. Avec une législation appropriée, le chargé interne de la protection des données peut être non seulement responsable à l'intérieur de l'entreprise pour la conformité de cette dernière mais il peut aussi avoir à rendre des comptes à l'extérieur, par exemple devant les autorités centrales de surveillance.

b) Examens de conformité et certification des sites Web par une tierce partie

Les examens de conformité réalisés par une tierce partie peuvent contribuer à faire en sorte que les sites Web agissent conformément à leurs déclarations en matière de protection de la vie privée. Le contrôle continu de conformité comprend généralement des « audits » périodiques sur les pratiques de traitement des informations et des « ensemencements » (on présente au site des informations à caractère personnel et on compare l'usage qui en est fait avec la politique déclarée par le site). Les sites qui satisfont continuellement à ces contrôles affichent une marque de certification, comme un label numérique²¹⁴ ou une icône

reconnue²¹⁵, confirmant au public qu'ils se conforment à leurs déclarations en matière de protection de la vie privée.

Un site Web peut demander des examens de conformité et une certification par une tierce partie pour différentes raisons. Les sites peuvent se soumettre de leur propre initiative à des examens de conformité. Par exemple, un site Web peut vouloir démontrer son attachement à la protection de la vie privée et apaiser les craintes des consommateurs que leurs informations à caractère personnel fassent l'objet d'une utilisation abusive. Le risque de retrait de la certification, et la publicité qui l'accompagnerait, peuvent constituer pour les sites Web une incitation suffisante à se conformer à leurs déclarations en matière de protection de la vie privée. En outre, les législations de protection de la vie privée ou les codes de conduite ou organes professionnels d'autorégulation²¹⁶ peuvent exiger que les entreprises en ligne se soumettent à une certification par une tierce partie.

Ci-après sont présentés des exemples d'entreprises et d'organisations professionnelles qui offrent des dispositifs de certification pour les pratiques de protection de la vie privée, et d'autres sont en cours de développement, comme BBB Online.

TRUSTe

TRUSTe est une organisation indépendante à but non lucratif qui certifie les sites Web satisfaisant aux exigences du programme *TRUSTe*²¹⁷. En particulier, un site Web doit : exposer ses pratiques de gestion des informations, se conformer aux pratiques ainsi déclarées et coopérer à tous les contrôles effectués par *TRUSTe*. Le site détermine lui-même le contenu de sa politique de protection de la vie privée mais, au minimum, sa déclaration doit révéler :

- Quel type d'informations le site collecte.
- Quel usage sera fait de ces informations ; et
- Avec qui (le cas échéant) il partagera ces informations.

TRUSTe a aussi annoncé récemment (juin 1998) que ses titulaires de licence seront tenus d'offrir aux consommateurs la possibilité de décider de l'usage qui peut être fait de leurs informations à caractère personnel, notamment concernant le transfert à des tiers.

Quand une entreprise a accepté les clauses du programme *TRUSTe* et a satisfait à l'examen initial de *TRUSTe*, elle est autorisée à arborer le label (*trustmark*) de *TRUSTe*. Pour faire en sorte que le site Web continue de respecter sa déclaration publique en matière de protection de la vie privée, le programme *TRUSTe* s'appuie sur un processus de contrôle permanent. En particulier, *TRUSTe* surveille la conformité d'un site Web aux pratiques qu'il a déclarées :

- En réexaminant périodiquement les sites participants.
- En « ensemencant » régulièrement les sites, c'est-à-dire en leur donnant des informations à caractère personnel et en vérifiant qu'il n'en est pas fait un usage contraire à la politique déclarée par le site ; et
- En organisant des « audits » de conformité sur site réalisés par des cabinets d'experts-comptables extérieurs.

Organismes de normalisation

Les organismes de normalisation sont un autre type d'organisation qui peuvent servir de tiers certificateurs en établissant des normes de protection de la vie privée et en offrant une certification officielle aux sites Web conformes. L'*Association canadienne de normalisation* (CSA) qui a établi un *Code type sur la protection des renseignements personnels* en est un exemple. La CSA souligne l'importance des audits indépendants réalisés par des vérificateurs certifiés pour l'audit de la protection de la vie privée, afin de vérifier la conformité de manière continue.

Cabinets d'experts-comptables

Les audits de la protection de la vie privée sont un des services qu'assurent maintenant les grands cabinets d'experts-comptables²¹⁸. Ces audits peuvent faire partie d'un dispositif de conformité établi par une organisation comme TRUSTe ou la CSA, ou ils peuvent être organisés directement par un cabinet d'experts-comptables. Le dispositif *WebTrust* offre un cadre permettant à un cabinet d'experts-comptables de fournir des services de certification²¹⁹. Créé par l'*American Institute of Certified Public Accountants* et l'*Institut canadien des comptables agréés*, le label de WebTrust a pour objet d'assurer aux consommateurs en ligne que le site Web participant obéit aux principes de WebTrust, notamment en matière de protection des informations. Pour surveiller et garantir en permanence la conformité aux principes de WebTrust, les experts-comptables spécialement autorisés effectuent régulièrement des examens de garantie. Aux États-Unis, les principes de l'*Individual Service Reference Group* prévoient des audits annuels par un cabinet d'experts-comptables extérieur.

c) Adhésion à des associations professionnelles

Les organismes professionnels qui imposent certaines pratiques de protection de la vie privée comme condition préalable à l'octroi de la qualité de membre peuvent contribuer à faire respecter ces pratiques sur les réseaux mondiaux. On peut citer à titre d'exemple : l'*Online Privacy Alliance* dans le cadre de l'appel pour la création de mécanismes tiers de certification (alliance transsectorielle créée en juin 1998 pour traiter les questions touchant à la protection de la vie privée en ligne, dont les membres sont convenus d'adopter, de mettre en œuvre et de déclarer leur politique de protection de la vie privée)²²⁰ ; l'*Internet Industry Association* australienne (qui a proposé un *Industry Code of Practice* avec une icône certifiant la conformité à ce code) ; et la *Direct Marketing Association* des États-Unis (association sectorielle, dont les membres mènent des activités de marketing par bases de données, qui encourage ses membres à afficher sur leurs sites Web leurs politiques de protection de la vie privée)²²¹. Par ailleurs, *BBBOnLINE*, dispositif de certification pour les entreprises en ligne adhérentes, envisage d'adopter une norme de protection de la vie privée parmi ses critères qualitatifs, éventuellement en établissant une charte distincte pour la protection de la vie privée représentée par un label ou une icône spécifique²²².

Les chances de réussite d'un organisme professionnel qui essaie de faire respecter des normes de protection de la vie privée dépendent d'un certain nombre de facteurs : la façon dont l'organisme fait connaître à ses membres le code de protection de la vie privée applicable, la manière dont l'organisme vérifie si ce code est suivi et la fréquence de ces vérifications, la façon dont l'organisme traite les plaintes des consommateurs et, quand il est constaté qu'un membre a enfreint le code, la manière dont ce dernier est sanctionné.

d) Autorités centrales de surveillance

La plupart des États qui ont une législation de protection de la vie privée établissent aussi une autorité centrale de surveillance telle qu'un office de la protection des données ou un commissaire à la protection de la vie privée, qui peuvent avoir les pouvoirs d'effectuer des audits préventifs de leur propre initiative.

Les « autorités de contrôle » mentionnées dans la directive de l'Union européenne²²³, par exemple, doivent pouvoir jouer ce rôle. En particulier, ces autorités sont investies de pouvoirs d'investigation (comme le droit d'accéder aux données) et de pouvoirs d'intervention (comme le droit d'interdire un traitement de données). Dans le cas de l'Union européenne, l'exercice de ces pouvoirs est soumis à une voie de recours judiciaire.

D'autres obligations légales peuvent être imposées pour faciliter la mission de surveillance de la conformité exercée par ces autorités centrales. Par exemple, un système d'enregistrement obligatoire augmente les informations dont disposent ces autorités²²⁴, et on peut exiger des audits initiaux pour s'assurer de la conformité à la loi avant la mise en oeuvre du traitement des données.

2. *Procédures de résolution des plaintes en cas d'infraction aux normes de protection de la vie privée*

Quand une personne pense que les principes de protection de la vie privée qui s'appliquent à ses relations avec un responsable de fichier particulier ont été enfreints, elle doit avoir accès à des voies de recours ou de réparation. Les procédures de résolution des plaintes en matière de protection de la vie privée qui existent dans les différents pays membres de l'OCDE varient à de nombreux égards.

Le traitement des plaintes en matière de protection de la vie privée peut varier selon que : *i*) la plainte se résout directement entre la personne concernée et le responsable de fichier, *ii*) la plainte est portée à la connaissance d'un organisme de certification tiers ou d'une association professionnelle, ou *iii*) des actions administratives, civiles ou pénales sont intentées.

Pour comparer ces catégories, on peut se poser des questions telles que :

- Quelle sorte de *réparation* la personne concernée peut-elle obtenir ? La réparation demandée peut être d'assurer la conformité aux principes de protection de la vie privée applicables (par exemple, en donnant accès aux données personnelles en question, en les corrigeant ou en inscrivant l'utilisateur sur une « liste orange » pour que ses données personnelles ne servent pas ultérieurement à des envois de publicités) ou peut aller jusqu'à des décisions d'indemnisation.
- De quelles *sanctions ultimes* dispose-t-on pour obliger le responsable du fichier à s'exécuter ? Les sanctions ultimes peuvent être des ordres de l'autorité centrale de surveillance, des décisions des tribunaux civils, des sanctions pénales (résultant d'une action intentée par la personne concernée, par l'autorité centrale de surveillance ou par une autre entité ayant des pouvoirs de poursuite), le retrait d'un label de certification ou l'exclusion d'une association professionnelle.
- Quel est le degré de formalisme et de complication de la procédure ? La résolution d'une plainte en matière de protection de la vie privée peut comporter différents degrés de formalisme : communications directes et informelles entre la personne concernée et le

responsable de fichier, ou médiation par l'autorité centrale de surveillance, jusqu'aux procédures judiciaires formelles.

a) Résolution des plaintes entre la personne concernée et le responsable de fichier

C'est généralement à l'auteur présumé de l'infraction que la personne concernée adresse initialement une plainte. En offrant des mécanismes destinés à recevoir et traiter les plaintes, les entreprises qui collectent et utilisent des informations susceptibles d'identifier la personne concernée peuvent être en mesure de résoudre beaucoup de litiges concernant la protection de la vie privée. La réparation obtenue directement du responsable de fichier est sans doute le moyen de résolution le plus rapide, le moins coûteux et le moins compliqué.

Les entreprises en ligne ont de bonnes raisons d'essayer de résoudre à l'amiable les plaintes de leurs clients concernant la protection de la vie privée. Ces motivations sont notamment les suivantes : protéger leur réputation, promouvoir de bonnes relations avec la clientèle et éviter que des procédures de réclamation plus formelles ne soient lancées.

Certaines entreprises en ligne proposent des procédures de traitement des plaintes clairement définies pour faciliter la résolution à l'amiable des plaintes en matière de protection de la vie privée. Ces dispositions peuvent par exemple spécifier les moyens de prendre contact avec l'organisation, les réparations offertes (par exemple, une indemnisation d'un montant fixé à l'avance en cas de violation de la vie privée) et les procédures pour faire arbitrer une réclamation.

Certaines dispositions de la législation ou des codes d'autorégulation imposent aux responsables de fichier de désigner des responsables internes de la protection des données pour faciliter la résolution des plaintes en offrant un interlocuteur précis avec des responsabilités bien définies.

b) Action par le biais des dispositifs de certification du secteur privé ou des associations professionnelles

Les dispositifs de certification et les associations professionnelles peuvent fournir des voies de recours pour les personnes qui se plaignent d'une violation de la vie privée par un site Web membre. Ces organisations sont utiles à deux égards. Premièrement, les critères de protection de la vie privée établis par le dispositif de certification ou l'association professionnelle constituent une référence par rapport à laquelle on peut juger les pratiques du responsable de fichier. Deuxièmement, il est de l'intérêt du certificateur tiers ou de l'association professionnelle, pour préserver sa réputation, de veiller à ce que ses membres se conforment à ses règles de protection de la vie privée et il possède généralement une force de négociation importante par rapport à ses membres. Ces facteurs donnent au certificateur tiers ou à l'association professionnelle à la fois la motivation et la capacité d'aider la personne concernée à faire aboutir sa plainte.

Les certificateurs tiers et les associations professionnelles peuvent jouer des rôles variés dans la résolution d'un litige concernant la protection de la vie privée, de l'investigation à la sentence, en passant par la médiation. La réparation peut consister en la soumission aux principes de protection de la vie privée applicables et en une indemnisation des dommages éventuels.

Les sanctions envisageables peuvent inclure :

- La publication du nom de l'entreprise sur une liste de « brebis galeuses ».
- Le retrait de l'icône de certification du site Web²²⁵.

- L'exclusion de l'association professionnelle²²⁶ ; et/ou
- Des poursuites administratives ou judiciaires contre le site Web (par exemple, pour violation de contrat ou usage illicite de marque).

Ci-après sont donnés des exemples de sociétés de certification et d'associations professionnelles qui peuvent jouer un rôle dans la résolution des plaintes des utilisateurs concernant les pratiques des sites Web à l'égard de la protection de la vie privée.

TRUSTe

Quand TRUSTe reçoit une plainte, cette organisation commence par envoyer une notification officielle et donne à l'auteur de l'infraction présumée une possibilité de répondre. Si cela ne donne pas satisfaction, TRUSTe conduit une enquête plus poussée. Suivant la gravité de l'infraction, l'enquête peut conduire à des pénalités, à un examen de conformité sur place ou au retrait du label du participant. Les cas graves peuvent être portés devant la FTC pour une action répressive en vertu du *Federal Trade Commission Act*, ou TRUSTe peut tenter une action en justice contre le site pour violation de contrat ou contrefaçon de marque.

L'Internet Industry Association d'Australie

En février 1998, l'*Internet Industry Association* australienne a publié un projet de code (*Industry Code of Practice*)²²⁷. Il est prévu qu'en première instance les plaintes se traiteront entre l'utilisateur et l'adhérent au Code dans un certain délai spécifié par le Code. En cas d'échec, le Code prévoit d'autres procédures, avec la désignation d'un médiateur et la possibilité, pour l'*Administrative Council* du Code, d'exiger de l'adhérent le respect du Code ou une publicité corrective et/ou le versement d'une indemnisation. Ce Conseil peut aussi retirer à un site l'autorisation d'utiliser son « symbole de conformité au Code ».

c) Actions administratives, civiles ou pénales

Les organes d'État peuvent apporter réparation sous la forme d'une décision administrative de l'autorité centrale de surveillance ou d'une décision judiciaire par les tribunaux. Les voies judiciaires peuvent être civiles (généralement avec l'attribution de dommages-intérêts et/ou des ordonnances de mise en conformité pour les infractions aux principes de la protection de la vie privée) ou pénales (avec des sanctions pénales contre les responsables de fichier en infraction).

Procédures administratives

Autorité centrale de surveillance

Il est souvent créé, dans les régimes de protection de la vie privée, une autorité centrale de surveillance (« Autorité de protection des données » ou « Commissaire à la protection de la vie privée »). Ces organismes offrent généralement un mécanisme administratif pour la résolution des plaintes en matière de protection de la vie privée.

L'intervention d'une autorité centrale de surveillance se justifie en partie par le fait que les personnes concernées peuvent ne pas avoir l'expertise ou les pouvoirs d'investigation nécessaires pour déterminer exactement quand ou par qui leur vie privée a été violée. Une Autorité de protection des données ou un

Commissaire à la protection de la vie privée apportera aussi son expérience et son autorité institutionnelle dans les tentatives de résolution des plaintes en matière de protection de la vie privée.

Les motifs permettant de porter plainte devant une autorité centrale de surveillance dépendent des termes de la législation qui lui confère ses pouvoirs, mais typiquement, les fondements des plaintes sont des infractions à la législation de la protection de la vie privée et, éventuellement, aux codes d'autorégulation ou à la déclaration de politique faite par l'entreprise en la matière.

Les pouvoirs d'une autorité centrale de surveillance spécifique et les types de réparation que peut obtenir la personne concernée dépendent aussi de cette législation fondatrice, mais ce genre d'institution est généralement investie du pouvoir :

- D'enquêter sur les plaintes.
- De conduire ou demander des audits.
- De tenter une conciliation entre les parties.
- D'entendre des témoins.
- D'émettre des recommandations.
- D'agir en tribunal spécialisé et de prononcer des décisions quasi-judiciaires comportant, par exemple, une indemnisation et des sanctions ; et/ou
- De renvoyer les plaintes, ou engager des poursuites, devant un tribunal judiciaire.

Dans de nombreux pays, les décisions de l'autorité centrale de surveillance peuvent faire l'objet d'un recours dans le système judiciaire ou devant un tribunal spécialisé (comme le *Data Protection Tribunal* au Royaume-Uni en ce qui concerne les mises en demeure du Registrar (enforcement notices)).

Autres organismes administratifs

D'autres organismes administratifs peuvent intervenir dans la résolution des plaintes en matière de protection de la vie privée. Quand le comportement qui fait l'objet d'une plainte comprend non seulement une atteinte aux principes de protection de la vie privée mais aussi aux règles de la loyauté du commerce, par exemple par la violation des engagements énoncés dans une déclaration de protection de la vie privée, une plainte peut alors être adressée aux organismes administratifs chargés de faire respecter ces autres pratiques. Aux Etats-Unis, par exemple, la FTC, en sa qualité d'autorité indépendante chargée de l'application de la loi, a de larges pouvoirs d'investigation et de décision concernant les plaintes contre les entreprises qui se livrent à des pratiques déloyales ou trompeuses²²⁸. Une entreprise (qu'il n'y a pas lieu de citer nommément) a récemment fait l'objet d'une enquête de la FTC pour avoir trompé ses clients sur l'utilisation de leurs informations à caractère personnel, qui a conduit à une décision transactionnelle.

Procédures civiles

Infractions à la législation de protection de la vie privée

Les législations de protection de la vie privée peuvent ouvrir aux personnes concernées un recours judiciaire contre les atteintes aux principes de protection de la vie privée établis par la loi²²⁹. La procédure prévoit généralement que ces plaintes sont portées devant les tribunaux par la personne lésée. De plus, dans certains pays de *Common Law*, des poursuites peuvent aussi être engagées sur la base d'un délit de violation de la vie privée.

Un tribunal peut disposer d'un large éventail de pouvoirs pour apporter une réparation appropriée dans une affaire donnée. Les décisions peuvent être notamment :

- D'ordonner un paiement pour indemnisation ou réparation.
- D'infliger une amende.
- De prononcer des ordonnances correctives (par exemple, pour permettre l'accès aux données personnelles en question ou les corriger).
- D'imposer ou interdire certaines pratiques dans le traitement des données ; et
- D'ordonner des contrôles périodiques pour s'assurer de la conformité.

Violations des déclarations, des accords en ligne ou des contrats régissant les flux transfrontières de données

L'éventail des voies de procédure civile dont dispose la personne concernée ne se limite pas à celui que l'on trouve dans la législation de protection de la vie privée. La législation générale relative aux violations de contrat, aux actes frauduleux et à la loyauté du commerce peut aussi s'appliquer quand le responsable de fichier a enfreint les termes de sa déclaration de politique de protection de la vie privée, d'un accord en ligne (comme les modalités et conditions associées à un formulaire d'inscription) ou d'un contrat régissant des flux transfrontières de données.

Un certain nombre de voies de recours de nature civile sont possibles en cas de violation d'une déclaration des politiques de vie privée ou d'un accord en ligne. Essentiellement, en notifiant ses pratiques en matière de protection de la vie privée, un site Web prend l'engagement de les suivre. Suivant la nature de l'infraction, la plupart des juridictions offrent des voies de recours au motif d'une présentation fallacieuse et/ou d'actes frauduleux si cet engagement est rompu.

Les visiteurs d'un site Web peuvent aussi disposer de voies de droit contractuelles. Il est très probable qu'il existe un contrat entre les parties quand elles ont conclu un accord en ligne, par exemple en acceptant explicitement les modalités mentionnées dans un formulaire d'inscription. Cependant, la distinction entre l'affichage d'une déclaration des pratiques de protection de la vie privée et un accord d'inscription en ligne est souvent une question de degré. Par exemple, le site Web peut contenir une section « Modalités et conditions » qui est formulée comme un contrat mais qui, à la différence d'un formulaire d'inscription, n'exige pas que l'utilisateur exprime explicitement son consentement²³⁰. Toutefois, en général, plus la formulation d'une mesure de protection de la vie privée ressemble aux termes d'un accord entre les parties, plus il y a de chances qu'il lui soit donné un effet contractuel et qu'elle ouvre des voies de droit pour violation de contrat. L'effet contractuel d'une clause de protection de la vie privée dépendra des autres termes du contrat (concernant, par exemple, la juridiction et l'arbitrage des différends) ainsi que du droit de la juridiction où on le considère.

La violation d'un contrat régissant des flux transfrontières de données par un responsable de fichier peut aussi fonder une action en justice pour la personne à laquelle se rapportent les données. Etant donné que cette personne n'est pas en général une partie au contrat, il peut exister des difficultés d'exécution dans les pays qui n'admettent pas la stipulation pour autrui. La solution adoptée dans le contrat Chemins de fer allemands - Citibank consiste à faire porter aux Chemins de fer allemands et à la filiale allemande de Citibank la responsabilité, à l'égard des personnes concernées en Allemagne, des violations de l'accord par leurs partenaires américains. De même, le Contrat-type du Conseil de l'Europe stipule que le préjudice occasionné à la personne concernée du fait de l'utilisation des données transférées ou en cas de résiliation du contrat doit être réparé par l'expéditeur des données en vertu du droit interne ou du droit international privé.

Arbitrage ou médiation

Le système judiciaire n'est pas le seul à offrir des voies de réparation civiles. Les parties peuvent suivre d'autres procédures de résolution des différends quand, par exemple, un contrat prévoit des audiences d'arbitrage. Le *Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données* du Conseil de l'Europe comme le *Contrat-type révisé* de la CCI (version provisoire de mai 1998) contiennent des clauses prévoyant l'arbitrage des différends entre le responsable de fichier expéditeur et le responsable de fichier destinataire.

Procédures pénales

Procédures reposant sur la législation de la protection de la vie privée

La législation de la protection de la vie privée peut établir des sanctions pénales pour les infractions graves²³¹. Une des raisons de l'existence de ces sanctions est de créer pour les entreprises une incitation à suivre de bonnes pratiques de protection de la vie privée plus forte que ce ne serait le cas si l'on se limitait à des condamnations au paiement de dommages-intérêts compensatoires quand il est fait la preuve d'une infraction est rapportée. L'éventail des entités admises à intenter des actions pénales (par exemple, la personne concernée, l'autorité de protection des données ou le ministère public) et la gamme de sanctions disponible (par exemple, peines d'amende ou d'emprisonnement) dépendent de la législation d'application²³².

Autres procédures pénales

Outre les poursuites pénales basées sur la législation de la protection de la vie privée, quand un responsable de fichier affirme faussement qu'il applique une certaine politique de protection de la vie privée, des poursuites peuvent être intentées en vertu de la législation sur la loyauté du commerce.

G. Éduquer les utilisateurs et le secteur privé

En raison de la nature du réseau d'information mondial, l'éducation des utilisateurs et des entités commerciales sur les questions relatives à la protection de la vie privée est un élément important pour cette protection. L'éducation apporte un complément à tous les autres instruments-guides et mécanismes mentionnés dans le présent Inventaire.

Les réseaux mondiaux transforment les entreprises en responsables de fichier. Du fait de la facilité avec laquelle on collecte et on transfère électroniquement les données, les commerçants en ligne sont amenés à manier beaucoup plus de données à caractère personnel, et beaucoup plus souvent, que s'ils étaient restés hors ligne. Des entités de plus en plus nombreuses sont ainsi amenées à agir en responsable de fichier soumis à la législation de la protection des données, aux codes de conduite ou aux normes d'autorégulation d'une branche d'activité. Plus ces fournisseurs de service Internet, commerçants en ligne, fournisseurs de contenu, concepteurs de navigateur ou exploitants de messagerie collective seront instruits des questions relatives à la protection de la vie privée, plus les pratiques de protection de la vie privée seront effectivement appliquées.

Les réseaux mondiaux soulèvent aussi, pour les utilisateurs, de nouvelles questions en matière de protection de la vie privée. La tendance que l'on voit apparaître à protéger les droits à la vie privée au moyen d'outils technologiques et par l'exercice d'un choix entre diverses options de protection de la vie privée implique que les utilisateurs ne seront pleinement protégés que s'ils sont assez compétents pour

veiller eux-mêmes à leurs intérêts. A la différence du monde hors ligne où il est rare qu'une personne doive porter attention aux implications de ses actions sur le plan de la protection de sa vie privée, un utilisateur en ligne doit être instruit des conséquences de ses allées et venues, de ses dires et de ses actions quand il est sur l'Internet. Par exemple, les utilisateurs doivent savoir quelles informations ils révèlent simplement en naviguant sur le Web, en envoyant un courrier électronique ou en affichant un message dans un groupe de discussion, quelles sont les conséquences de l'accord qu'ils donnent à certaines options de protection de la vie privée, comment utiliser les technologies protectrices de la vie privée et comment configurer leurs préférences dans leur logiciel de navigation pour obtenir le degré de protection souhaité.

Outre les méthodes traditionnelles d'éducation du public dans les écoles, sur le lieu de travail et dans les médias,²³³ divers sites Web offrent des conseils en ligne sur la protection de la vie privée dans les réseaux mondiaux. Ces sites sont entretenus par *i*) des organisations internationales, comme le Conseil de l'Europe²³⁴ ; *ii*) des organismes gouvernementaux, comme la FTC aux Etats-Unis²³⁵, beaucoup d'autorités centrales de surveillance dans d'autres parties du monde²³⁶ et *iii*) des organisations du secteur privé, comme le *Project OPEN (Online Public Education Network)*, la *Direct Marketing Association*²³⁷ des Etats-Unis, le *Center for Democracy and Technology*²³⁸, l'*Electronic Privacy Information Center*²³⁹, *Call for Action* et TRUSTe²⁴⁰. On peut utiliser des liens hypertexte pour donner accès, à partir des sites Web qui collectent des informations à caractère personnel, à ces sources d'information sur la protection de la vie privée.

NOTES

1. Les Sections I et II ont été mises à jour pour tenir compte des changements intervenus dans certains pays (mais pas tous) jusqu'en janvier 2003.

En avril 1999, les faits nouveaux suivants ont été portés à l'attention du Secrétariat :

- Le 21 avril 1999, la Pologne a signé la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données (Convention no. 108).
 - Le 26 avril 1999, 50 fournisseurs de services Internet ont adhéré au réseau *Freedom Network*, un collectif international d'opérateurs de serveurs indépendants qui fournissent des technologies de protection de la vie privée des utilisateurs du Web. Les 50 prestataires et réseaux indépendants sont situés en Australie, en Autriche, au Canada, aux États-Unis, au Japon, aux Pays-Bas et au Royaume-Uni (voir www.zeroknowledge.com/partners).
2. Ces informations, et en particulier l'adresse de courrier électronique de l'utilisateur, sont potentiellement suffisantes pour retrouver le nom et l'adresse réels de la personne en question au moyen d'un annuaire du courrier électronique (voir, par exemple, l'annuaire Four11 à www.bfm.org/misc/four11.com.html).
 3. Chaque ordinateur sur l'Internet a une adresse IP qui lui est propre, de la forme #.#.#.# (où chaque # est un nombre de 0 à 255).
 4. Pour un exposé sur les « cookies », voir www.cookiecentral.com/.
 5. Les « cookies » sont utiles parce qu'ils permettent à un utilisateur et à un site Web d'interagir au fil du temps. Par exemple, si un utilisateur passe commande d'un disque de musique sur une certaine page, cette information peut être consultée quand l'utilisateur arrive à la page de paiement. Les « cookies » permettent aussi à un site de reconnaître un utilisateur particulier quand il revient ultérieurement visiter ce site. Chaque fois que l'utilisateur revient, le site peut récupérer des informations précises sur l'utilisateur, comme la langue de préférence, le mot de passe ou les centres d'intérêts et préférences de l'utilisateur déterminés par les articles ou documents auxquels cet utilisateur a accédé au cours de ses visites précédentes.
 6. L'article 27 de la directive de l'Union européenne note que les États membres devraient établir des mécanismes pour la mise en place de codes de conduite destinés « à contribuer à la bonne application » des dispositions nationales en matière de protection des données.
 7. C'est la définition des « données de caractère personnel », paragraphe 1, Annexe à la Recommandation du Conseil.
 8. Paragraphes 2 et 3, Annexe à la Recommandation du Conseil.
 9. Paragraphes 15 à 18, Annexe à la Recommandation du Conseil.
 10. Paragraphes 20 à 22, Annexe à la Recommandation du Conseil.
 11. Paragraphe 19, Annexe à la Recommandation du Conseil.
 12. Parmi les travaux récents ou en cours du Comité PIIC (en plus du présent Inventaire) on peut mentionner : un rapport intitulé « Mise en œuvre dans l'environnement électronique, et en particulier sur Internet, des Lignes directrices de l'OCDE sur la protection de la vie privée » (octobre 1997) ; une Conférence de l'OCDE sur la « Protection de la vie privée dans une société de réseaux mondialisée » (février 1998) et le rapport qui en a résulté (juillet 1998) ; un rapport de consultant analysant les résultats d'une enquête de l'OCDE sur le Web ; et une Déclaration ministérielle sur la protection de la vie privée dans les réseaux mondiaux (issue de la Conférence ministérielle, *Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial* (Ottawa, 7-9 octobre 1998)).

13. Chiffres en décembre 1997. Le Tableau des instruments nationaux montre les pays membres de l'OCDE qui ont ratifié la Convention 108.
14. La signature de la Convention représente un engagement politique, plutôt que juridique. Toute Partie peut étendre ou restreindre le champ d'application de la Convention 108 en adressant une déclaration au Secrétaire général du Conseil de l'Europe lors de la signature ou de la ratification.
15. Article 6, Convention 108.
16. Article 12.3(a), Convention 108.
17. Article 13.2, Convention 108.
18. Article 4, Convention 108.
19. Partie A, paragraphe 5, Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel.
20. Cela inclut les responsables de traitement établis en un lieu où la loi d'un Etat membre s'applique en vertu du droit public international, ou qui recourent à des moyens situés sur le territoire d'un Etat membre (sauf si ces moyens ne sont utilisés qu'à des fins de transit).
21. Articles 3 et 4, directive de l'Union européenne.
22. L'article 8 de la directive de l'Union européenne interdit le traitement des données sensibles, avec certaines exceptions telles que le consentement explicite de la personne concernée.
23. Articles 10, 11 et 12, directive de l'Union européenne.
24. Articles 18 à 21, directive de l'Union européenne.
25. Article 14, directive de l'Union européenne.
26. Articles 22 à 24, directive de l'Union européenne.
27. Article 1(2), directive de l'Union européenne.
28. Article 25(1), directive de l'Union européenne.
29. Article 26, directive de l'Union européenne.
30. Article 28, directive de l'Union européenne.
31. Articles 22 à 24, directive de l'Union européenne.
32. Voir www.wto.org/.
33. Article XIV(c)(ii), Partie II, AGCS.
34. Pour plus d'informations, voir à <http://europa.eu.int/comm/dg15/en/media/dataprot/news/santen.htm>
35. Le « Groupe institué par l'article 29 » de l'Union européenne fait référence à ce document dans une recommandation de décembre 1997.
36. L'ISO a été créée en 1947. Voir www.iso.ch/.
37. Au sein de l'ISO, d'autres organes mènent actuellement des travaux sur la protection de la vie privée : JTC1 (Comité technique mixte), SC27 (Sous-comité travaillant sur la sécurité des données), TAG12 (Groupe technique consultatif) et un Comité de l'ISO sur l'informatique médicale.
38. Voir www.iccwbo.org/.
39. Voir www.iccwbo.org/home/menu_advert_marketing.asp pour plus d'information.
40. Voir www.epic.org/.
41. Voir www.cdt.org/.
42. Voir www.privacy.org/.

43. Voir www.PrivacyExchange.org/.
44. Loi du 20/12/1990 sur la protection des données. Le texte de cette loi est disponible en anglais sur le site du Commissaire à la protection des données de Berlin : www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm.
45. Article 21(1).
46. Articles 43 et 44.
47. Réglementation fédérale (en allemand) disponible à www.datenschutz-berlin.de/recht/de/rv/index.htm.
48. Aussi désigné par l'abréviation IuKDG (01.8.1997) ; un résumé est disponible à www.iukdg.de.
49. Voir www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf. On trouvera plus d'informations sur le site www.iukdg.de.
50. On peut trouver les adresses des autorités de protection des données des Länder à www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm.
51. La conférence du 29 avril 1996 présente les éléments essentiels pour la réglementation en matière de protection des données dans les services en ligne. Voir www.datenschutz-berlin.de/sonstige/konferen/sonstige/old-res2.htm.
52. La version la plus récente de la nouvelle loi fédérale (en allemand) est disponible à www.datenschutz-berlin.de/themen/ds-allg/bdsg_neu.htm.
53. On trouvera le texte de cette loi à l'adresse suivante : <http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm>.
54. Adresse du site web du Commissaire : www.privacy.gov.au.
55. On trouvera sur le site www.privacy.gov.au/links/index.html#2 des liens vers les divers régimes des Etats et territoires.
56. On trouvera un registre des codes approuvés au site suivant : www.privacy.gov.au/business/codes.
57. Les dispositions concernant les transferts internationaux sont entrées en vigueur le 1^{er} juillet 1987.
58. Journal officiel fédéral I n° 100/1997.
59. Journal officiel fédéral autrichien n° 194/1994.
60. Le texte (en allemand) peut être téléchargé sur le site Web du Parlement (www.parlinkom.gv.at/). Ce lien amène à www.parlinkom.gv.at/pd/pm/XX/bis/016/101613.html. Le texte officiel en allemand et la traduction non officielle en anglais de la loi fédérale sur la protection des données, de même que les traductions en anglais d'autres textes, sont disponibles gratuitement auprès de la *Datenschutzkommission* par courrier électronique (Contacter georg.lechner@bka.gv.at). L'ensemble de la législation autrichienne est disponible sur Internet en allemand (www.ris.bka.gv.at).
61. Voir www.privacy.fgov.be/.
62. Articles 37 à 43.
63. Document disponible à www.lachambre.be.
64. Document disponible à www.ispa.be/fr/c040201.html.
65. Document disponible à <http://laws.justice.gc.ca/en/p-21/93445.html>.
66. Pour l'Alberta, voir *Freedom of Information and Protection of Privacy Act* (1995) ; Colombie-Britannique : *Freedom Of Information and Protection of Privacy Act* (1993) ; Manitoba : *Freedom of Information and Protection of Privacy Act* (1998) ; Nouveau-Brunswick : *Protection of Personal Information Act* (1998) ; Terre-Neuve : *Freedom of Information Act* (1982) ; Territoires du Nord-Ouest : *Access to Information and Protection of Privacy Act* (1997) ; Nouvelle-Ecosse : *Freedom of Information and Protection of Privacy Act* (1993) ; Ontario : *Loi sur l'accès à l'information et la protection de la vie*

- privée* (1988) et *Loi sur l'accès à l'information municipale et la protection de la vie privée* (1991) ; Québec : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (1982) ; Saskatchewan : *Freedom of Information and Protection of Privacy Act* (1991) et *Local Freedom of Information and Protection of Privacy Act* (1993) ; et Yukon : *Access to Information and Protection of Privacy Act* (1996). On peut trouver des informations sur toutes les lois de protection de la vie privée au Canada à <http://infoweb.magi.com/~privcan/other.html>.
67. Voir, par exemple, au Manitoba, le *Personal Health Information Act* (1997).
 68. Ce Comité réunissait des représentants de l'industrie et du gouvernement canadien.
 69. CAN/CSA-Q830-96. On peut consulter ou commander cette norme de la CSA à : www.csa-intl.org/onlinestore/welcome.asp?Language=EN.
 70. Publication PLUS 8300 (décembre 1996). On peut commander ce document sur le site Web de la CSA : www.csa-intl.org/onlinestore/welcome.asp?Language=EN.
 71. Document disponible à www.caip.ca/. Des associations comme l'Association canadienne de la technologie de l'information et l'Association canadienne de l'informatique ont aussi établi des codes pour les technologies de l'information.
 72. Loi 5/92 du 29 octobre 1992. Ce document est disponible en ligne à www.ag-protecciondatos.es/datmen.htm. En 1993, un Décret royal a été adopté qui complète (entres autres) les dispositions sur les flux transfrontières de données, les procédures d'enregistrement et les droits des personnes concernées.
 73. Voir www.ag-protecciondatos.es.
 74. Articles 43 et 44 de la loi.
 75. Loi n° 28/94.
 76. Code disponible (en espagnol) à www.aece.org/default.asp.
 77. 5 U.S.C. § 552a (1994).
 78. Voir www.ibiblio.org/nii/NII-Task-Force.html.
 79. Document disponible à www.ntia.doc.gov/ntiahome/privwhitepaper.html#B11.
 80. Document disponible à www.ntia.doc.gov/reports/privacydraft/198dftprin.htm.
 81. Document disponible à www.ftc.gov/reports/privacy3/index.htm.
 82. Déposition de Robert Pitofsky, Président de la FTC, au Congrès, 21 juillet 1998. Document disponible à www.ftc.gov/os/1998/07/privac98.htm.
 83. Voir www.itic.org/.
 84. Les principes de l'ITIC reposent de manière générale sur les Lignes directrices de l'OCDE, avec des dispositions spéciales sur « l'éducation du marché » et « l'adaptation des pratiques de protection de la vie privée aux technologies électroniques et en ligne ».
 85. Voir www.privacyalliance.org/. Parmi ses membres figurent Microsoft, AOL, AOL Time Warner, Sun Microsystems, Dell, Ernst & Young et Yahoo!.
 86. Voir www.the-dma.org/.
 87. Voir www.bbb.org/alerts/carupr.asp pour plus d'informations.
 88. Voir www.finlex.fi/pdf/saadkaan/E9990523.PDF.
 89. Voir www.tietosuoja.fi.
 90. Articles 47-48, loi sur les données à caractère personnel.
 91. Voir www.ssml-fdma.fi.

92. Articles 226-16 à 226-24.
93. Voir www.cnil.fr.
94. Dispositions pénales établies par les articles 41 à 44 de la loi 78/17, et article 226-21 du Code pénal français.
95. Loi n° 92-1446 du 31 décembre 1992.
96. Loi n° 95-73 du 21 octobre 1995.
97. Document disponible à <http://users.info.unicaen.fr/~herve/publications/1997/charte/charte.final.html>.
98. Les Acteurs de l'Internet qui s'engagent à respecter la charte sont principalement des utilisateurs et des fournisseurs de service Internet basés sur le territoire français.
99. Code de déontologie sur la protection des données à caractère personnel.
100. Traduction anglaise, *Journal officiel de la République hellénique*, Volume 1, n° 50 du 10 avril 1997.
101. La mission de l'Autorité de protection des données grecque est spécifiée dans l'article 19 de la loi.
102. Articles 11 à 14.
103. Article 23.
104. Article 21.
105. Article 22.
106. Loi n° LXIII de 1992. Cette loi a été modifiée par les Lois n° LXV et LXXVI de 1995.
107. Articles 11 à 15.
108. Article 27. Le Commissaire à la protection des données a des pouvoirs répressifs conformément aux articles 25 et 26.
109. Articles 17 et 18.
110. Le droit à la protection de la vie privée est interprété comme étant un des droits individuels non spécifiés de l'article 40(3) de la Constitution.
111. Sections 21 à 23.
112. IDMA *Code of Practice on Data Protection* (3 mai 1995).
113. Article 33.
114. Article 14(1).
115. Article 22.
116. Article 33.
117. Articles 37 à 39.
118. Voir, par exemple, Préfecture de Kanagawa, Ordonnance du 26 mars 1990.
119. Ces Lignes directrices ont été publiées à l'origine en avril 1989.
120. Articles 22 et 23 des Lignes directrices.
121. L'ENC est une organisation professionnelle gérée par la *New Media Development Association*, organisation auxiliaire du MITI. Voir www.nmda.or.jp/enc/index-english.html.
122. Voir www.ecom.or.jp/.
123. Document disponible à www.telesa.or.jp/e_guide/e_guid01.html.
124. 31 mars 1979.

125. L’Autorité de contrôle, établie par une loi du 9 août 1993, se compose du Procureur d’Etat et du Secrétaire général et deux membres de la Commission consultative.
126. Articles 32 à 39.
127. Voir les Lois n° 65 du 20 août 1993 et n° 74 du 2 octobre 1992.
128. Projet de loi 4357.
129. Article 214, Code pénal du District fédéral.
130. Voir www.datilsynet.no/.
131. Sections 97 à 109, *Privacy Act*.
132. Voir www.privacy.org.nz/top.html. Les fonctions du *Commissioner* sont énoncées dans la Section 13 du *Privacy Act*.
133. Sections 46-53, *Privacy Act*.
134. Section 85, *Privacy Act*.
135. Document disponible à www.internetnz.net.nz/icop/icop99the-code.html.
136. Document disponible à www.privacy.org.nz/top.html.
137. Document disponible à www.privacy.org.nz/comply/justice.html.
138. Wet van 6 juli 2000, Stb. 302, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). Une traduction anglaise non officielle de ce texte est accessible sur le site Web de l’Autorité de protection des données, www.cbppweb.nl.
139. Wet van 19 oktober 1998, Stb.610, houdende regels inzake de telecommunicatie (Telecommunicatiewet).
140. Aux termes de l’article 51 :
- (1) Aucune personne ne peut être contrainte, sauf si la loi l’exige, de révéler des informations sur elle-même.
- (2) Les autorités publiques ne doivent pas acquérir, collecter ni rendre accessibles d’autres informations sur les citoyens que ce qui est nécessaire dans un Etat démocratique régi par la loi.
- (3) Toute personne a le droit d’accéder aux documents et collections de données officiels la concernant. La loi peut établir des limitations de ces droits.
- (4) Toute personne a le droit d’exiger la correction ou la suppression des informations fausses ou incomplètes, ou des informations acquises par des moyens contraires à la loi.
- (5) Les principes et procédures régissant la collecte des informations et l’accès aux informations seront spécifiés par la loi.
141. 29 août 1997, Dz.U. nr 133, poz. 833. La loi est entrée en vigueur le 30 avril 1998.
142. Articles 50 à 54.
143. Loi n° 10/91, modifiée en 1994 par la loi n° 28/94 pour renforcer la protection des données sensibles et des données dans les flux transfrontières entre les parties à la Convention 108.
144. Article 8(h).
145. Articles 27, 29 et 30.
146. Articles 34 à 41.
147. Loi 109/91 du 17 août 1991.
148. Décret-loi 296/94 du 24 décembre 1994.

149. Décret-loi 1/95 du 12 janvier 1995. Il existe aussi un Décret-loi 48/97 sur les cartes d'identité du Système national de santé.
150. Décret réglementaire 2/95 du 25 janvier 1995.
151. Décrets réglementaires 4/95 et 5/95 du 31 janvier 1995.
152. Décret réglementaire 27/95 du 31 octobre 1995.
153. Loi n° 256/1992.
154. Le *Ministère de l'Intérieur* et l'*Office tchèque des télécommunications* coopèrent avec l'*Office pour le système d'information de l'Etat* à la préparation du projet de loi.
155. Loi complétée par des décrets de 1987, 1990 et 1997. Le *Data Protection Act* est disponible à www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm.
156. Voir www.lcd.gov.uk/foi/datprot.htm.
157. Pour une synthèse de la loi, voir www.hmso.gov.uk/acts/acts1990/Ukpga_19900037_en_1.htm#end.
158. Pour une synthèse de la loi, voir www.hmso.gov.uk/acts/acts1993/Ukpga_19930010_en_1.htm#end.
159. Pour une synthèse de la loi, voir www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm.
160. Pour plus d'informations, voir <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm>.
161. Pour le texte complet de la loi, voir www.hmso.gov.uk/acts/acts1998/19980042.htm.
162. Pour le texte complet de la loi, voir www.hmso.gov.uk/acts/acts1998/19980029.htm.
163. Voir www.ispa.org.uk/.
164. Par exemple, l'*Advertising Association* (publicité), le *Code of the Banking Practice Review Committee* (banque) et le *Code for Computer Bureau Services* de la *Computing Services Association* (services informatiques).
165. *Tryckfrihetsförordningen* (loi N° 1949:105). – Cette loi, comme les autres textes législatifs suédois, projets de loi gouvernementaux, etc, sont accessibles via Internet à www.riksdagen.se/rixlex/index_en.htm.
166. *Regeringsformen* (loi N° 1974:152).
167. Loi N° 1998:204.
168. Le Décret sur la protection des données de caractère personnel. (loi N° 1998:1191).
169. *Yttrandefrihetsgrundlagen* (loi N°1991:1469).
170. 19 juin 1992.
171. Voir www.edsb.ch/.
172. Article 11 de la LPD.
173. Article 23 de la LPD.
174. Articles 28 et 28f, Code civil (SR 210).
175. Dans le monde hors ligne, l'anonymat est un moyen important (bien que souvent considéré comme allant de soi) de protection de la vie privée. Par exemple, on peut acheter en espèces pour éviter qu'il se crée un relevé des transactions, on peut exprimer des opinions controversables sous un pseudonyme et, souvent, des garanties d'anonymat sont offertes pour encourager certaines personnes (informateurs de la police, sources journalistiques ou dénonciateurs de scandale) à révéler des informations.
176. Voir <http://internet.junkbuster.com/>
177. Voir www.thelimitsoft.com/cookie.html.
178. Voir www.hotmail.com/.

179. Voir www.gilc.org/speech/anonymous/remailer.html.
180. Cela comprend généralement l'adresse IP de l'utilisateur, le nom de domaine et sa localisation géographique, le système d'exploitation et le navigateur utilisés, la page Web visualisée juste avant l'accès au présent site et éventuellement l'adresse de courrier électronique de l'utilisateur.
181. Voir www.anonymizer.com/.
182. L'intermédiaire peut prendre diverses mesures pour empêcher les abus de l'anonymat. Par exemple, l'Anonymizer bloque l'accès à certains sites, comme les salons de bavardage, où des abus ont eu lieu dans le passé. En outre, *Infonex*, qui exploite le service Anonymizer, enregistre pour chaque utilisateur un relevé de son adresse IP, de son nom d'hôte et des documents demandés. Ces informations peuvent éventuellement être communiquées et contribuer à identifier l'utilisateur si (1) l'*Anonymizer* est utilisé pour perturber un service, par exemple en inondant d'un contenu importun une adresse de courrier électronique ou un groupe de discussion ou (2) si une décision judiciaire ordonne la communication de ces informations.
183. Plus de 50 systèmes de paiement différents ont été proposés pour l'Internet. Pour une liste, voir <http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html>
184. Voir www.mondex.com/.
185. Une carte à puce est une petite carte qui contient un microprocesseur. La carte Mondex a été programmée pour fonctionner comme un « porte-monnaie électronique » dans lequel on peut charger un certain montant et que l'on peut utiliser pour payer des biens ou services ou pour faire un transfert vers une autre carte Mondex au moyen de lecteurs de carte.
186. Voir www.engage.com.
187. Voir www.doubleclick.com/.
188. Voir www.click-stream.com/webfaw.html
189. On peut arguer que ces informations ne sont pas en elles-mêmes des données à caractère personnel puisqu'elles ne se relient pas « à une personne physique identifiée ou identifiable » [article 1(b), Lignes directrices de l'OCDE)], mais ce sont certainement des données *potentiellement* personnelles dans la mesure où la liaison avec l'identité de la personne concernée peut s'effectuer si, par exemple, elle communique son nom à la compagnie qui tient les profils ou à un commerçant à qui le profil a été fourni.
190. Par exemple, d'après une enquête de la FTC portant sur 1 200 sites Web commerciaux aux Etats-Unis (mars 1998), seulement 14% présentaient un quelconque avertissement sur leurs pratiques en matière de collecte d'informations (voir www.ftc.gov/reports/privacy3/survey.htm). De même, d'après une enquête sur les 100 sites Web les plus importants réalisée en juin 1997 par l'Electronic Privacy Information Center (EPIC), seulement 17% de ces sites avaient une politique explicite de protection de la vie privée (voir www.epic.org/reports/surfer-beware.html).
191. Voir www.truste.org/.
192. Voir www.bbonline.org/.
193. Voir www.privacyalliance.org/.
194. Voir www.aeanet.org.
195. On examine le système TRUSTe de manière plus détaillée dans la section où l'on décrit les moyens de faire respecter les principes de protection de la vie privée.
196. On peut trouver à travers tout le Web des exemples d'affichage des politiques de protection de la vie privée. Voir, par exemple, les déclarations sur la protection de la vie privée de Lego (www.lego.com/eng/info/privacypolicy.asp), Continental Airlines (www.continental.com/travel/policies/privacy/default.asp?SID=1DED319A40994D1BA93200181E79A5EB), Australian Legal Information Institute (www.austlii.edu.au/austlii/privacy.html), ZDNet (www.zdnet.com/findit/privacy.html), DoubleClick (www.doubleclick.com/company_info/about

- [doubleclick/privacy/](#)), Reader's Digest ([www.rd.com/privacy.jhtml](#)) et Microsoft ([www.microsoft.com/info/privacy.htm](#)).
197. Voir, par exemple, les sites Web de *The Economist* ([www.economist.co.uk/](#)) et du *Financial Times* ([www.ft.com/](#)) qui exigent l'inscription de l'utilisateur avant qu'il puisse accéder à une quelconque partie du site, à l'exception des premières pages.
198. Voir [www.w3.org/P3P/](#).
199. PICS est un exemple de plate-forme technologique capable d'assurer un étiquetage numérique. PICS a été conçu par le W3C comme un cadre structurant l'étiquetage du contenu des pages Web, qui permet aux utilisateurs (ou aux parents d'enfants qui utilisent le Web) de fixer des règles de filtrage bloquant de manière sélective l'accès à certain types de contenu. Cependant, on peut appliquer le protocole PICS d'autres manières. Ainsi, en élaborant un vocabulaire des étiquettes de protection de la vie privée, la méthode PICS peut aussi servir à étiqueter les pratiques des sites Web dans ce domaine. Pour un exemple de ce type de vocabulaire, voir Joel R. Reidenberg, « The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection » dans *Lex Electronica*, Vol.3, n° 2 ([www.lex-electronica.org/reidenbe.html](#)).
200. Pour une appréciation des conditions auxquelles devrait satisfaire une plate-forme technique de protection de la vie privée telle que P3P, voir le « Report of the Groupe de travail international sur la protection des données dans les télécommunications » contenu dans l'Annexe 4 du compte rendu de la 23^{ème} réunion du Groupe de travail, 14-15 avril 1998 à Hong Kong, Chine.
201. Pour la version la plus récente du protocole P3P (juillet 1998), voir [www.w3.org/TR/P3P](#).
202. Voir [www.moniker.com](#).
203. MatchLogic gère les sites Web suivants : [www.grandgobosh.com](#), [www.excite.com](#), [www.webcrawler.com](#) et [www.quicken.com](#).
204. Ces termes désignent une liste de personnes qui ne souhaitent pas recevoir les courriers de prospection des entreprises de vente directe et à laquelle ces entreprises doivent obéir. L'Autriche offre un exemple d'adoption de ce genre de système dans la loi [voir la Section 268(8) du *Code des entreprises* (1994), journal officiel fédéral autrichien n° 194/1994].
205. Cette technique permettant de « se faire rayer » des listes de publipostage électronique peut s'appliquer de manière plus générale. Par exemple, on a annoncé aux Etats-Unis un site *World Wide Web* consacré à la faculté de refus. Ce site ([www.consumer.gov/](#)), entretenu par la *Federal Trade Commission*, donne des indications sur la façon dont une personne peut empêcher les entreprises de consulter les fiches de renseignements sur sa solvabilité, s'opposer à la vente des informations afférentes au permis de conduire ou faire rayer son nom et son adresse des listes de prospection commerciale.
206. La DMA assure actuellement le fonctionnement de dispositifs similaires pour le refus des sollicitations par le courrier postal et par téléphone. Pour un exemple de dispositif opérationnel concernant le courrier électronique, voir [http://preference.the-dma.org/products/empssubscription.shtml](#).
207. Voir [www.doubleclick.net/us/corporate/privacy/privacy/default.asp?asp_object_1=&](#).
208. L'article 26(2) de la directive de l'Union européenne reconnaît explicitement la possibilité d'utiliser des contrats entre les responsables de fichier pour faire en sorte que les données à caractère personnel transférées d'un pays à un autre reçoivent une « protection adéquate » selon les termes de cette directive.
209. Le Contrat-type prévoit que les personnes concernées pourront faire valoir des droits d'accès, de rectification et d'effacement auprès du destinataire des données (clause 2) et que l'expéditeur des données devra résilier le contrat ou engager la procédure d'arbitrage si ces droits sont refusés. En outre, le préjudice occasionné à la personne concernée du fait de l'utilisation des données ou en cas de résiliation du contrat doit être réparé par l'expéditeur des données en vertu du droit interne ou du droit international privé (paragraphes 36 et 41 du rapport explicatif).
210. Voir le site Web de la CCI à [www.iccwbo.org](#).

211. En particulier, le groupe de travail est d'avis qu'il faut imposer au destinataire des données les règles de fond du pays expéditeur en matière de protection des données et que, pour rendre ces règles effectives, il faut réunir les éléments suivants : assurer un niveau satisfaisant de respect des règles, fournir une assistance aux personnes concernées dans l'exercice de leurs droits et offrir des voies de recours appropriées en cas de violation de ces droits.
212. Les mécanismes de conformité et de réparation ne sont pas indépendants. Par exemple, l'existence de voies de recours efficaces améliore le degré de conformité aux normes de protection de la vie privée. En effet, plus la probabilité de punition est grande pour une entreprise qui viole les normes de protection de la vie privée, moins elle est encline à commencer à violer ces normes. Toutefois, étant donné la complexité des techniques modernes du traitement de données et les obstacles (comme le coût) auxquels doivent faire face les personnes qui veulent faire valoir leurs droits, une combinaison de mécanismes préalables et *post facto* a le plus de chances d'être efficace pour assurer le degré de protection de la vie privée désiré.
213. Voir, par exemple, la loi allemande de 1990 sur la protection des données, le Principe 1 du Code type de l'Association canadienne de normalisation (voir le paragraphe 91) et les Lignes directrices du MITI au Japon (voir paragraphe 166).
214. Ce genre d'étiquette pourrait être utilisé dans le système P3P.
215. Il existe diverses méthodes, comme l'authentification numérique, pour empêcher l'utilisation non autorisée de ces icônes de certification. Voir www.verisign.com/index.html.
216. Voir, par exemple, l'*Online Privacy Alliance* qui « soutient les dispositifs de tierce partie qui attribuent un symbole identifiable indiquant aux consommateurs que le propriétaire ou exploitant d'un site Web, service en ligne ou autre espace en ligne a adopté une politique de protection de la vie privée qui contient les éléments formulés par l'*Online Privacy Alliance*, a mis en place des procédures pour assurer la conformité à cette politique et permet la résolution des plaintes des consommateurs ». Voir www.privacyalliance.org/resources/enforcement.shtml
217. Voir www.truste.org/
218. Ces 15 dernières années, les cabinets d'experts-comptables ont étendu leur champ d'activité, au-delà du simple audit des performances financières d'une entreprise, à l'audit des performances de l'entreprise dans un éventail de domaines de la « responsabilité sociale » (par exemple, l'impact environnemental des activités d'une entreprise).
219. Voir www.aicpa.org/assurance/trustservices/index.asp?.
220. Voir www.privacyalliance.org/.
221. Pour un examen de ce dispositif et un rapport critique sur la faible proportion des nouveaux membres qui se conforment à cette recommandation, voir « *Surfer Beware II: Notice Is Not Enough* », par l'*Electronic Privacy Information Center* (<http://www2.epic.org/reports/surfer-beware2.html>).
222. Voir www.bbbonline.org/.
223. Article 28 de la directive de l'Union européenne, qui stipule que chaque État membre devra avoir une « autorité de contrôle » investie de larges pouvoirs d'investigation, de réparation et de poursuite.
224. Voir, par exemple, l'obligation de notification stipulée par l'article 18 de la directive de l'Union européenne.
225. Comme le proposent, par exemple, TRUSTe et l'*Internet Industry Association* australienne.
226. Voir, par exemple, le *Code de protection de la vie privée* établi par l'*Association canadienne du marketing direct* qui prévoit l'exécution des dispositions par une procédure d'audiences de l'ACMD et la possibilité d'exclure l'entreprise de l'association.
227. Les principes nationaux peuvent s'appliquer dans les environnements en ligne ou électroniques. En mai 1998, le *Online Council* auquel participent les Ministères chargés des TI au niveau fédéral, des États et des territoires, a reconnu que ces principes formaient une base de référence nationale pour des normes de protection de la vie privée.

228. Pour un exposé sur les pouvoirs répressifs de la FTC concernant « les pratiques ou actes déloyaux ou trompeurs » en vertu de la Section 5(a) du *Federal Trade Commission Act*, voir www.ftc.gov/ogc/brfovrwv.htm. On notera que la juridiction de la FTC est limitée par la condition que les pratiques incriminées « causent, ou risquent de causer aux consommateurs un *préjudice substantiel* que les consommateurs eux-mêmes ne sont pas raisonnablement en mesure d'éviter et qui n'est pas compensé par des effets bénéfiques supérieurs pour les consommateurs ou pour la concurrence » (15 U.S.C. Sec. 45(n)) (italiques ajoutées).
229. Voir, par exemple, les articles 22 et 23 de la directive de l'Union européenne.
230. Voir, par exemple, le site Web canadien *Sympatico* (<http://www1.sympatico.ca/>).
231. C'est ce qu'envisage, par exemple, l'article 24 de la directive de l'Union européenne.
232. Par exemple, aux Etats-Unis, le *Fair Credit Reporting Act* impose des sanctions pénales à quiconque obtient des rapports d'endettement sous des motifs fallacieux.
233. Voir, par exemple, *Easy i* qui publie à l'usage des entreprises des vidéos et des logiciels éducatifs concernant la protection de la vie privée (www.easyi.com/products/hwc.asp).
234. Voir www.coe.int.
235. Voir www.ftc.gov/privacy/index.html.
236. Voir, par exemple, les sites Web officiels de l'Australie (www.privacy.gov.au/), de la France (www.cnil.fr/), de l'Espagne (<https://www.agenciaprotecciondatos.org>) et du Royaume-Uni (www.ukonline.gov.uk/Home/Homepage/fs/en).
237. Voir www.the-dma.org/.
238. Voir www.cdt.org/privacy/topten/online.html.
239. Voir www.epic.org/privacy/.
240. Voir www.truste.org/partners/users_primer.html.

RÉFÉRENCES

- COE (Conseil de l'Europe) (1980), « Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 18 septembre 1980 », <http://conventions.coe.int/Treaty/FR/WhatYouWant.asp?NT=108&CM=1&DF=21/07/03>.
- COE (2001), « Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », ETS n° 108, <http://conventions.coe.int/treaty/FR/Treaties/Html/181.htm>.
- DMA (Direct Marketing Association) (1998), « Testimony of the DMA before the Subcommittee on Communications, Committee on Commerce, Science and Transportation of The United States Senate », 17 juin, www.the-dma.org.
- Dix, Alexander (1996), « The German RailwayCard: A Model Contractual Solution of the 'Adequate Level of Protection' Issue ? », 18^{ème} International Privacy and Data Protection Conference, Ottawa, Canada, 18-20 septembre 1996, www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm.
- Froomkin, Michael (1996), « The Essential Role of Trusted Third Parties in Electronic Commerce », 75 Oregon L. Rev. 49.
- Goldberg, Ian, David Wagner et Eric Brewer (1997), « Privacy-Enhancing Technologies for the Internet », www.cs.berkeley.edu/~daw/papers/privacy-comcon97-www/privacy-html.html.
- International Working Group on Data Protection in Telecommunications (1996), « Budapest-Berlin Memorandum », www.datenschutz-berlin.de/diskus/13_15.htm.
- Kang, Jerry (1998) « Information Privacy in Cyberspace Transactions », 50 Stan. L. Rev. 1193-1294, en 1224-1230.
- NU (Nations Unies) (1990), « The United Nations High Commissioner for Human Rights' Guidelines for the Regulation of Computerised Personal Data Files », Resolution 45/95 de 14 décembre 1990, www.unhchr.ch/html/menu3/b/71.htm.
- NU (1997) « Question du suivi des principes directeurs pour la réglementation des fichiers personnels informatisés : rapport du Secrétaire général établi conformément à la décision 1995/114 de la Commission [des droits de l'homme] », Rapport E/CN.4/1997/67 du Conseil économique et social, 23 janvier.
- OCDE (1980) *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, Paris, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

UE (Union Européenne) (1995), « Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data », OJ n° L281 de 23/11/1995, 31, Parlement Européen et le Conseil, Bruxelles.

UE (1997a), « Document de réflexion DG XV WP 4 », adopté par le Groupe le 26 juin 1997.

UE (1997b), « Directive 97/66/EC », Parlement Européen et le Conseil, Bruxelles.

UE (1998), « Évaluation des codes d'autoréglementation sectoriels : quand peut-on dire qu'ils contribuent utilement à la protection des données dans un pays tiers ? » DG XV WP 7, adopté par le Groupe le 14 janvier 1998.