Protection de la vie privée en ligne

ORIENTATIONS POLITIQUES ET PRATIQUES DE L'OCDE

OCDE

Protection de la vie privée en ligne

Orientations politiques et pratiques de l'OCDE

OCDE

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

En vertu de l'article 1er de la Convention signée le 14 décembre 1960, à Paris, et entrée en vigueur le 30 septembre 1961, l'Organisation de Coopération et de Développement Économiques (OCDE) a pour objectif de promouvoir des politiques visant :

- à réaliser la plus forte expansion de l'économie et de l'emploi et une progression du niveau de vie dans les pays membres, tout en maintenant la stabilité financière, et à contribuer ainsi au développement de l'économie mondiale ;
- à contribuer à une saine expansion économique dans les pays membres, ainsi que les pays non membres, en voie de développement économique ;
- à contribuer à l'expansion du commerce mondial sur une base multilatérale et non discriminatoire conformément aux obligations internationales.

Les pays membres originaires de l'OCDE sont : l'Allemagne, l'Autriche, la Belgique, le Canada, le Danemark, l'Espagne, les États-Unis, la France, la Grèce, l'Irlande, l'Islande, l'Italie, le Luxembourg, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède, la Suisse et la Turquie. Les pays suivants sont ultérieurement devenus membres par adhésion aux dates indiquées ci-après : le Japon (28 avril 1964), la Finlande (28 janvier 1969), l'Australie (7 juin 1971), la Nouvelle-Zélande (29 mai 1973), le Mexique (18 mai 1994), la République tchèque (21 décembre 1995), la Hongrie (7 mai 1996), la Pologne (22 novembre 1996), la Corée (12 décembre 1996) et la République slovaque (14 décembre 2000). La Commission des Communautés européennes participe aux travaux de l'OCDE (article 13 de la Convention de l'OCDE).

Also available in English under the title:

Privacy Online
OECD GUIDANCE ON POLICY AND PRACTICE

AVANT-PROPOS

Vie privée en ligne : orientations politiques et pratiques s'adresse aux pays membres de l'OCDE, aux entreprises industrielles et commerciales et aux particuliers. Il a été réalisé sous l'égide du Comité de la politique de l'information, de l'informatique et des communications (Comité PIIC de l'OCDE) par son Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP).

Centrées sur la mise en œuvre des Lignes directrices de l'OCDE sur la vie privée, les orientations politiques et pratiques proposées dans ce volume sont fondées sur les travaux réalisés par l'OCDE en application de la Déclaration ministérielle de 1998 concernant la protection de la vie privée sur les réseaux mondiaux. Cette publication répond à un objectif majeur de l'OCDE : établir des passerelles entre les stratégies suivies par les différents pays pour assurer la protection efficace de la vie privée et des données à caractère personnel, sans entraver les flux internationaux de données à caractère personnel sur les réseaux mondiaux.

Cet ouvrage, conçu pour renforcer l'impact et accroître la visibilité de l'action de l'OCDE et pour souligner l'importance de ses Lignes directrices sur la vie privée dans l'élaboration et la mise en œuvre d'une combinaison de solutions pour assurer une protection des données à caractère personnel au niveau mondial et la libre circulation de l'information, s'articule comme suit :

- La première partie présente un résumé des travaux réalisés par le GTSIVP entre 1998 et 2002.
- La deuxième partie propose des orientations politiques et pratiques élaborées à partir de ces travaux.
- La troisième partie comprend l'ensemble des documents et instruments (par exemple les outils Internet) recensés dans la première partie.

C'est Anne Carblanc qui a orchestré ce travail au sein de l'OCDE, en tant que secrétaire et conseillère du GTSIVP et du Comité PIIC.

L'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 dans le chapitre 6 a été préparé par le secrétariat avec les contributions reçues des pays membres, des organisations internationales et régionales et du Comité consultatif économique et industriel auprès de l'OCDE (BIAC).

Le contenu du Générateur de déclaration de politique de protection de la vie privée en ligne présenté au chapitre 7a été préparé par le secrétariat avec les contributions reçues des pays membres, des organisations internationales et régionales et du Comité consultatif économique et industriel auprès de l'OCDE (BIAC), qui a également recruté des entreprises pour tester le Générateur. Des autorités chargées de la protection des données [notamment au Canada, à Hongkong (Chine), en Nouvelle-Zélande et au Royaume-Uni], des groupes représentant les intérêts des consommateurs et des experts en matière de protection des consommateurs (notamment le Centre pour la défense de l'intérêt public au Canada et le Conseil des consommateurs au Danemark) ont fait part de leurs conseils et de leur expérience. L'outil lui-même a été développé par le secrétariat, notamment son Service de technologies de l'information et des communications, avec le soutien de DaimlerChrysler et de Microsoft. Les assistants de protection de la vie

privée en cours de développement par TRUSTe, AT&T et la DMA ont été d'une aide précieuse dans les premières étapes du développement du Générateur. On tient à souligner les contributions de James Palmer, Rachael Wellby, Amanda Chandler et Steve Fuzesi, ainsi que l'aide apportée par Joachim Schlette, Alfred Büllesbach et Christian Lallemand dans l'élaboration du Générateur. Peter Lübkert, du secrétariat de l'OCDE a fourni des conseils et l'assistance technique de sa division. Julie Harris, également du secrétariat de l'OCDE, a contribué à la production de cet ouvrage.

Les chapitre 9 et 10 ont été préparé par le secrétariat avec des contributions du Comité de politique des consommateurs et le GTSIVP. On tient à remercier particulièrement le gouvernement néerlandais pour une contribution spéciale au travail présenté dans le chapitre 10.

Le chapitre 11 à été préparé par un consultant, M. Chris Kuner de la firme Hunton & Williams, sur la base de contributions des pays membres et sous la direction du secrétariat.

Mme Lauren Hall, ancien vice-président exécutif de la *Software & Information Industry Association*, et actuellement Directrice de la politique technologique, *Advanced Strategy and Policies*, Microsoft Corporation a rédigé le chapitre 12 en tant que consultant à l'OCDE et en collaboration avec le secrétariat.

Le chapitre 13 rend compte du forum de l'OCDE sur les technologies protectrices de la vie privée et inclut en appendice deux études de consultants réalisées pour le compte de l'OCDE . Le premier est M. Laurent Bernat, Directeur de Projetweb, l'autre de M. Perri 6, Directeur du *Policy Programme* à *l'Institute for Applied Health and Social Policy*, du King's College (Londres).

Le chapitre 14 est le fruit d'une collaboration entre un certain nombre d'experts et de consultants. Il a bénéficié de contributions des pays membres de l'OCDE, d'organisations internationales et régionales, ainsi que du BIAC. En particulier, le secrétariat tient à remercier Mme Elizabeth Longworth, avocate, partenaire principale chez *Longworth Associates* (Nouvelle-Zélande), qui a rédigé la première version du rapport, et à mentionner le concours que lui ont apporté Mme Lorraine Brennan, directrice du département Arbitrage, propriété intellectuelle et conseil juridique, du *U.S. Council for International Business*, M. Alexander Dix, Commissaire à la protection des données et à l'accès à l'information du *Land* de Brandebourg (Allemagne) et M. Ian Lloyd, professeur de droit des technologies de l'information et directeur du *Centre for Law, Computers and Technology* de l'Université de Strathclyde (Royaume-Uni).

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE.

TABLE DES MATIÈRES

POINTS SAILLANTS

Coopération internationale pour instaurer la confiance en ligne

Depuis la Conférence ministérielle d'Ottawa de 1998, les pays membres de l'OCDE s'attachent, en coopération étroite avec des représentants des entreprises, de l'industrie, des consommateurs et de la société civile, à établir des passerelles entre les différentes approches adoptées au plan national pour assurer une protection réelle et efficace de la vie privée en ligne et instaurer la confiance dans le commerce électronique entre entreprises et consommateurs, sur la base des Lignes directrices de l'OCDE sur la vie privée. Étant donné le caractère mondial des technologies de réseau, la coopération internationale est essentielle pour la protection transfrontière de la vie privée et des données à caractère personnel en ligne.

Établir des passerelles et combiner des approches

Il existe désormais un large consensus sur le rôle important que joue la protection de la vie privée pour susciter la confiance à l'égard de l'environnement en ligne. La protection efficace de la vie privée en ligne et la garantie de la circulation transfrontière des données à caractère personnel sont deux objectifs que partagent les différents pays. Toutefois, les pays membres ont diverses vues sur les moyens d'atteindre ces objectifs. Ils s'accordent cependant à considérer qu'il n'y a pas de solution unique. En combinant des approches fondées sur la réglementation ou l'autorégulation et qui associent des instruments juridiques, techniques et éducatifs adaptés au contexte juridique, culturel et social dans lequel elles doivent opérer, on peut espérer apporter des solutions efficaces qui, au-delà de l'établissement de passerelles, contribuent à véritablement intégrer différents éléments en des solutions viables. Une participation résolue et complémentaire des pouvoirs publics, des entreprises et des utilisateurs ou groupes de consommateurs (« les participants ») est également indispensable au succès de cette combinaison de mesures relatives à la vie privée : tous ont un rôle à jouer pour aider à promouvoir le respect d'une protection adéquate de la vie privée sur les réseaux mondiaux, et partant, renforcer la confiance dans le commerce électronique.

Moyens politiques et pratiques pour renforcer la protection de la vie privée en ligne

Quatre ans après Ottawa, l'action en faveur de la protection de la vie privée en ligne s'est traduite par une évolution des pratiques des sites Web dans ce domaine. Même si des améliorations sont encore nécessaires, les progrès à ce jour dans la protection de la vie privée en ligne sont encourageants. Tous les participants devront continuer de s'engager activement en faveur de politiques et pratiques qui concourent à une protection efficace de la vie privée en ligne. Principalement destiné aux pays membres de l'OCDE, ce rapport propose des orientations politiques et des mesures pratiques utiles pour l'ensemble des participants, pour aider à assurer la protection de la vie privée au niveau mondial, sur la base des Lignes directrices de l'OCDE. Il vise également à accroître la sensibilisation aux problèmes et aux mesures de protection de la vie privée en ligne.

Une étape dans un processus continu

Parce que l'innovation technologique est permanente dans l'environnement Internet et que le caractère mondial des systèmes et les échanges d'information influent constamment sur l'évolution des cultures et perceptions nationales en matière de vie privée, ce rapport ne doit pas être considéré comme l'aboutissement des travaux de l'OCDE dans ce domaine. Il constitue plutôt une étape dans la conduite de ces travaux pour promouvoir le respect de droits importants et l'ouverture des économies et sociétés et en particulier pour assurer, avec la circulation des flux transfrontières de données à caractère personnel, une protection efficace de la vie privée sur les réseaux mondiaux.

Partie I

RÉSUMÉ DES TRAVAUX DE L'OCDE DESTINÉS À ASSURER LA PROTECTION DE LA VIE PRIVÉE

Chapitre 1

INTRODUCTION

Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée

Les Lignes directrices de l'OCDE régissant la protection de la vie privée se sont imposées comme les principes essentiels pour la protection internationale de la vie privée.

La Recommandation relative aux Lignes directrices de l'OCDE régissant la protection de la vie privée a été adoptée par le Conseil de l'OCDE le 23 septembre 1980[1]. Les huit principes énoncés sont les suivants :

- Limitation en matière de collecte.
- Qualité des données.
- Spécification des finalités.
- Limitation de l'utilisation.
- Garanties de sécurité.
- Transparence.
- Participation individuelle.
- Responsabilité.

Les Lignes directrices de 1980 sur la vie privée sont toujours reconnues comme représentant un consensus international sur les normes en matière de vie privée et comme donnant les orientations nécessaires pour la collecte de données à caractère personnel, quel que soit le support considéré. Elles sont toujours considérées comme ayant défini les fondements de la protection de la vie privée sur les réseaux mondiaux.

La protection de la vie privée dans la société mondiale de l'information

Le développement des technologies numériques de l'informatique et des réseaux, et notamment de l'Internet, s'est accompagné de la promesse de retombées sociales et économiques du fait de la facilitation des échanges d'informations, de la possibilité de création de nouveaux produits et de services et de l'élargissement du choix du consommateur. Cependant, l'intégration des réseaux mondiaux dans la vie quotidienne et la poursuite des innovations technologiques multipliant les possibilités de recueil de données à caractère personnel ont eu pour effet simultanément d'accroître les avantages d'une adaptation personnalisée aux besoins du consommateur et d'accentuer les craintes concernant la protection de la vie privée et des données à caractère personnel.

Dans l'économie du numérique, les personnes peuvent laisser derrière elles des « empreintes » électroniques ou des enregistrements des « lieux » qu'elles ont visités, des sujets qu'elles ont consultés, des pensées qu'elles ont formulées, des messages qu'elles ont envoyés et des biens et services qu'elles ont achetés. Cela pose des problèmes de vie privée dans la mesure où toutes ces données à caractère personnel exploitables sur ordinateur, qu'elle aient été générées de façon automatique ou non, sont susceptibles d'être recueillies, mémorisées, détaillées, individualisées, croisées ou exploitées pour divers usages dans des lieux géographiquement dispersés partout dans le monde, éventuellement à l'insu du consommateur ou sans son consentement.

Le contexte du mandat ministériel

Compte tenu des travaux de l'OCDE ayant conduit à la rédaction des Lignes directrices de 1980 et de la poursuite des travaux sur la protection de la vie privée, l'Organisation a été considérée comme une enceinte appropriée afin de promouvoir un dialogue entre pouvoirs publics, entreprises et industries, utilisateurs et consommateurs et autorités responsables de la protection des données pour :

- Aborder les questions liées à la protection de la vie privée et aux flux transfrontières de données à caractère personnel en relation avec les réseaux mondiaux.
- Examiner diverses solutions qui pourraient faciliter l'application généralisée d'une protection de la vie privée en ligne et contribuer à l'édification d'un environnement de confiance pour le développement du commerce électronique.

C'est à la conférence de l'OCDE sur « Le démantèlement des obstacles au commerce électronique mondial », tenue à Turku (Finlande) du 19 au 21 novembre 1997, que le respect de la vie privée en ligne a fait l'objet pour la première fois d'une large attention politique. La vie privée, la sécurité et la protection des consommateurs ont alors été considérées comme des éléments essentiels pour susciter la confiance dans l'environnement en ligne, condition *sine qua non* du développement du commerce électronique.

Un petit nombre de thèmes majeurs liés à la protection de la vie privée dans le contexte des réseaux mondiaux d'information et de communication ont été dégagés lors de l'Atelier de l'OCDE sur « La protection de la vie privée dans une société de réseaux mondialisée », tenue à Paris les 16 et 17 février 1998. L'atelier a notamment mis en lumière la nécessité de permettre aux individus de prendre des décisions appropriées concernant leurs données à caractère personnel, la question clé de la libre circulation des données, le besoin d'instruments flexibles et efficaces de protection de la vie privée, le potentiel offert par les solutions technologiques, le besoin de moyens de sanction et de voies de recours et la nécessité d'une meilleure éducation.

Ces thèmes ont été affinés et développés pendant la préparation de la Conférence de l'OCDE au niveau Ministériel « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial » qui a eu lieu à Ottawa du 7 au 9 octobre 1998. Lors de cette conférence, les Ministres ont adopté une Déclaration sur la protection de la vie privée sur les réseaux mondiaux[2] et lancé dans ce domaine des actions qui devaient être poursuivies les années suivantes.

Déclaration ministérielle

La Déclaration ministérielle de 1998 d'Ottawa reconnaissait que « les principes technologiquement neutres énoncés dans les Lignes directrices de 1980 régissant la protection sur la vie privée continuent de refléter un consensus international sur les orientations qui doivent guider la collecte et la manipulation des données à caractère personnel sur quelque support que ce soit, et fournissent une base sur laquelle fonder la protection de la vie privée sur les réseaux mondiaux ».

Les Ministres ont réaffirmé « leur engagement à l'égard de la protection de la vie privée sur les réseaux mondiaux, afin d'assurer le respect de droits importants, de construire la confiance dans les réseaux mondiaux et d'empêcher les restrictions inutiles aux flux transfrontières de données à caractère personnel ». Ils sont convenus de prendre les mesures nécessaires pour assurer, par diverses mesures spécifiées, la mise en œuvre efficace des Lignes directrices de l'OCDE sur la vie privée en ce qui concerne les réseaux mondiaux. Ils ont chargé l'OCDE d'examiner les problèmes spécifiques soulevés par la mise en œuvre des Lignes directrices en relation avec les réseaux mondiaux et de fournir aux pays membres des orientations pratiques en la matière.

Les Ministres sont également convenus de faire le point des progrès accomplis dans la réalisation des objectifs de leur Déclaration dans un délai de deux ans, et d'évaluer le besoin de nouvelles actions pour assurer la protection des données à caractère personnel sur les réseaux mondiaux, dans le cadre de ces objectifs. Les progrès dans la réalisation des objectifs de la Déclaration ministérielle d'Ottawa ont fait l'objet d'un rapport en 1999 au Forum de Paris et en 2001 à Doubaï lors du Forum pour les économies de marché émergentes.

Plan d'action de l'OCDE

Les initiatives approuvées par les Ministres à la Conférence de l'OCDE ont été intégrées dans le Plan d'action de l'OCDE et assignées aux comités et groupes de travail compétents[3]. Dans ce contexte, le GTSIVP, sous les auspices du Comité de la politique de l'information, de l'informatique et des communications (PIIC) a axé une bonne partie de ses travaux sur la mise en œuvre des éléments du Programme de travail de l'OCDE en six points en faveur de la protection de la vie privée en ligne :

- Encourager l'adoption de politiques à l'égard de la vie privée.
- Encourager la notification en ligne des politiques à l'égard de la vie privée à l'attention des utilisateurs.
- Faire en sorte que des mécanismes de contrainte et de recours soient disponibles en cas de non-respect.
- Promouvoir l'éducation et la sensibilisation des utilisateurs à la protection de la vie privée en ligne et aux moyens d'assurer cette protection.
- Encourager l'utilisation de technologies protégeant la vie privée.
- Encourager l'utilisation et le développement de solutions contractuelles pour les flux transfrontières de données en ligne.

Tous les documents et autres instruments (par exemple outils sur Internet) produits par le GTSIVP et rendus publics par le Comité PIIC sont joints au présent rapport (Voir la partie III). Ils forment le matériel de base sur lequel s'appuie la partie II consacrée aux orientations générales et pratiques.

NOTES

1. Voir le chapitre 4. La Recommandation concernant les Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel a été adoptées par le Conseil de l'OCDE le 23 septembre 1980.

2. Voir le chapitre 5.

3. (*i)* Le GTSIVP a mené sous les auspices du Comité PIIC des travaux sur la protection de la vie privée et des données à caractère personnel ; sur les infrastructures et technologies sécurisées, l'authentification et la certification ; et sur la cryptographie (au titre du thème A du Plan d'action – « Renforcer la confiance des utilisateurs et consommateurs ») ; (*ii)* le GTSIVP a également travaillé en collaboration avec le Comité de la politique à l'égard des consommateurs (CPC), lequel s'est occupé des aspects du commerce électronique liés à la protection des consommateurs (sous le thème A du Plan d'action) ; (*iii)* le Comité des affaires fiscales a travaillé sur les questions de fiscalité (sous le thème B du Plan d'action – « Établir les règles fondamentales pour le marché numérique ») ; (*iv)* le Comité des échanges a travaillé sur la politique commerciale et les aspects du commerce électronique liés à l'accès au marché (sous le thème B du Plan d'action) ; *v)* le Groupe de travail sur les politiques en matière de télécommunications et de services d'information a travaillé sous les auspices du Comité PIIC sur l'accès à l'infrastructure d'information et sur son utilisation (sous le thème C du Plan d'action – « Améliorer l'infrastructure de l'information pour le commerce électronique ») ; (*vi)* le Comité de la gestion publique s'est attaché à renforcer la sensibilisation mondiale au problème de l'an 2000 (sous le thème C du Plan d'action) ; (*vii)* le Comité PIIC a travaillé sur les implications pour les pouvoirs publics des incidences économiques et sociales du commerce électronique mondial (sous le thème D du Plan d'action – « Optimiser les avantages du commerce électronique ») ; (*viii)* le Comité d'aide au développement s'est attaché à assurer une participation mondiale (sous le thème D du Plan d'action) ; (*ix)* le Comité de l'industrie (devenu depuis le Comité de l'industrie et de l'environnement de l'entreprise) a travaillé sur le commerce électronique et les PME (sous le thème D du Plan d'action) ; (*x)* le Centre pour la recherche et l'innovation dans l'enseignement a travaillé sur les didacticiels et le multimédia (sous le thème D du Plan d'action).

Chapitre 2

EXÉCUTION DU MANDAT MINISTÉRIEL : TRAVAUX DE L'OCDE

Ce chapitre résume des différents aspects des travaux de l'OCDE destinés à assurer la protection de la vie privée en ligne.

Chapitre 2

EXÉCUTION DU MANDAT MINISTÉRIEL : TRAVAUX DE L'OCDE

Les pays membres de l'OCDE ont adopté une approche pragmatique pour donner suite au mandat Ministériel. Leurs travaux ont privilégié fortement l'éducation, le recueil d'informations juridiques et techniques, la collecte et la diffusion d'exemples d'initiatives et d'expériences dans la mise en œuvre des Lignes directrices, la mise en place d'un forum de discussion, l'élaboration d'un outil fondé sur la technologie Internet et l'exploration et l'analyse d'un certain nombre d'instruments et mécanismes à caractère juridique et technique destinés à assurer la protection de la vie privée en ligne.

Les pays membres ont dans un premier temps recensé, aux niveaux international, régional et national, l'éventail des instruments juridiques, des pratiques et des technologies, soit en usage soit en cours de développement, permettant de mettre en œuvre et de faire appliquer les principes de protection de la vie privée dans l'environnement en ligne. Cet inventaire[1] a notamment couvert les textes législatifs à caractère général ou sectoriel régissant la protection des données, les codes de conduite, les normes industrielles et les solutions technologiques à l'initiative de l'industrie, notamment les technologies protectrices de la vie privée, les outils pédagogiques en ligne, les systèmes de labellisation, de certification et d'apposition de marques relatives à la vie privée, ainsi que les mécanismes de règlement des litiges. Il a été noté que des outils technologiques étaient de plus en plus utilisés pour protéger les droits à la vie privée en ligne. Il a également été souligné qu'une protection efficace de la vie privée en ligne exige des utilisateurs des réseaux non seulement de posséder une certaine « culture informatique » mais aussi d'avoir conscience des répercussions de leurs actions sur la protection de la vie privée.

1) Encourager l'adoption de politiques en matière de vie privée

Les pays membres de l'OCDE ont élaboré un Générateur de déclarations de politique de protection de la vie privée (le « Générateur »)[2], qui est un instrument pédagogique utilisant la technologie Internet et offrant aux organisations un soutien et des orientations pour l'élaboration de politiques et de pratiques compatibles avec les Lignes directrices de l'OCDE sur la vie privée. Le Générateur est notamment conçu pour aider les organisations à élaborer des politiques et déclarations relatives à la protection de la vie privée et à les rendre accessibles sur leurs sites Web.

Le Générateur de l'OCDE permet aux organisations de revoir leurs pratiques courantes en matière de vie privée grâce à un questionnaire sur les pratiques qu'elles appliquent. Un projet de déclaration de politique est alors créé par le Générateur, qui donne une idée de la mesure dans laquelle les pratiques de l'organisation se conforment aux Lignes directrices de l'OCDE sur la vie privée. Ce projet de déclaration constitue une base qui peut être ensuite amendée ou développée en fonction des besoins, de manière à refléter précisément les pratiques de l'organisation en matière de vie privée dans le cadre d'un processus conduisant à la définition d'une déclaration définitive. Le Générateur peut être adapté pour tenir également compte de questions préoccupant plus particulièrement certains pays membres. Il propose également des liens vers des organisations utiles des secteurs public et privé.

Les pays membres ont noté que, du moins dans certains pays, l'affichage d'une politique en matière de vie privée rendra une organisation juridiquement responsable de toute action en contravention avec cette politique. Dans tous les cas, la déclaration elle-même devra être évaluée par rapport aux exigences de la législation nationale. En tout état de cause, l'existence du Générateur devrait faciliter les efforts nationaux pour encourager les entreprises à adopter des politiques en matière de vie privée, qu'elles soient ou non tenues de le faire de par la loi.

Les pays membres ont également considéré que l'utilisation du Générateur devrait contribuer à une plus grande cohérence dans la protection de la vie privée au-delà des frontières nationales. Il peut aider les organisations à comprendre les exigences liées aux principes de protection de la vie privée aux niveaux national et international et à établir un climat de confiance avec les autres organisations et les utilisateurs individuels en ligne. Il peut aider aussi les utilisateurs individuels à prendre l'habitude de consulter les déclarations de politique de protection de la vie privée lorsqu'ils visitent des sites en ligne.

2) Encourager la notification en ligne aux utilisateurs des politiques à l'égard de la vie privée

En rendant gratuitement disponible le Générateur de déclarations de politique de protection de la vie privée, l'OCDE a contribué à sensibiliser aussi bien les entreprises que les utilisateurs individuels aux questions de protection de la vie privée en ligne. Grâce au Générateur, les entreprises peuvent plus aisément informer en ligne les utilisateurs individuels de leurs politiques à l'égard de la vie privée[3]. L'ajout de liens vers des sites Web gouvernementaux et privés vise à mieux faire connaître aux entreprises et autres organisations, ainsi qu'aux utilisateurs et consommateurs, le cadre qui régit la protection de la vie privée dans leurs activités en ligne.

En approuvant le Générateur, les pays membres ont fait un pas en avant décisif pour promouvoir l'ouverture et la confiance dans le commerce électronique parmi les visiteurs des sites Web.

Le fait que le public perçoit positivement les déclarations en ligne de politiques en matière de vie privée est confirmé par quelques sondages d'opinion et d'enquêtes. Ainsi, une étude réalisée en 2000 a montré que 75 % des utilisateurs et consommateurs avaient tendance à faire davantage confiance aux commerçants en ligne qui affichaient sur leurs sites Web des déclarations de politique en matière de vie privée[4]. De même, une étude de mai 2002[5] a conclu que le manque à gagner dans les ventes en ligne d'ici 2006 pourrait atteindre USD 24.5 milliards du fait de politiques inadaptées en matière de vie privée : « Si une entreprise pratique des politiques inadaptées en matière de vie privée en ligne, ses ventes hors ligne pourraient également reculer au profit de concurrents plus attentifs aux questions de protection de la vie privée », selon les auteurs du rapport. Depuis 1997 toutefois, parmi les sites Web commerciaux la pratique consistant à poster des déclarations de politique en matière de vie privée pour renforcer la confiance sur les réseaux tend à se généraliser. En mars 2002, la *Progress and Freedom Foundation*[6] a indiqué que 98 % des 100 sites les plus fréquemment visités affichaient des déclarations de politique en matière de vie privée et que 88 % des sites étudiés de façon aléatoire affichaient également de telles déclarations.

3) Faire en sorte que des mécanismes de contrainte et de recours soient à la disposition des utilisateurs en cas de non-respect des principes et politiques de protection de la vie privée

Les pays membres de l'OCDE ont achevé plusieurs projets consacrés aux questions des mécanismes de recours, de mise en œuvre et de sanction, dans le contexte des opérations transfrontières en ligne. Il convient de relever plus particulièrement à cet égard les mécanismes de règlement alternatif des litiges (RAL) en ligne ainsi que diverses autres méthodes de mise en œuvre et de sanction qui vont au-delà des approches réglementaires traditionnelles.

Le règlement alternatif des litiges

Les pays membres de l'OCDE ont entrepris une série d'études sur le RAL, qui consiste à recourir à des méthodes pratiques extrajudiciaires faisant appel à des tiers neutres pour un règlement rapide et à faible coût des litiges. En décembre 2000, l'OCDE[7], conjointement avec la Conférence de droit international privé de La Haye et la Chambre de commerce internationale (CCI), a tenu à La Haye une conférence sur « Les mécanismes alternatifs de règlement des litiges en ligne applicables aux litiges visant la protection de la vie privée et des consommateurs »[8]. Le but de cette conférence était d'explorer si, et dans quelle mesure, les mécanismes de RAL en ligne pouvaient aider à régler les litiges entre entreprises et consommateurs suscités par les problèmes de protection de la vie privée et de protection des consommateurs, et donc améliorer la confiance dans le commerce électronique mondial. La conférence portait avant tout sur les petits litiges, de même que sur les systèmes flexibles et non officiels offrant une solution de compromis adéquate compte tenu de la nature du litige et du type de processus de résolution (par exemple, négociation assistée et médiation).

Un consensus s'est dégagé sur certains principes, tels que : la solution la plus efficace consiste à régler les litiges le plus tôt possible ; la souplesse et la diversité des mécanismes de RAL sont précieuses ; des progrès technologiques appropriés pourraient faciliter le RAL ; les individus ont besoin d'informations sur les procédures pour pouvoir participer efficacement ; les mesures de protection en matière de procédure sont importantes dans certains litiges.

La conférence a été suivie par un programme de travail centré sur les aspects juridiques et pédagogiques du RAL. Il s'agissait avec le volet du programme sur les aspects juridiques de procéder à un tour d'horizon des régimes juridiques des pays membres, applicables au RAL dans les relations entreprises-consommateurs, de manière à voir si les dispositions juridiques en vigueur avaient une incidence sur le recours au RAL en ligne, et de quelle manière. Un rapport[9] a été établi à partir des réponses des pays membres à une enquête sur les lois et règlements en vigueur concernant le RAL. Ce rapport a montré qu'il n'y avait pas d'ensemble unique de règles régissant le RAL. Différentes règles ont été élaborées, en fonction du contexte. Dans un certain nombre de secteurs, le cadre juridique en vigueur donne des orientations pour les parties susceptibles d'engager une procédure de RAL au niveau national. Ainsi, de nombreux pays réglementent la prestation de services d'arbitrage. Toutefois, les réglementations visant à régir de façon générale la prestation de services de RAL moins officiels dans le cadre du commerce entreprises-consommateurs sont peu nombreuses. Les réglementations en place visent généralement la fourniture de services de RAL dans le cadre de mécanismes établis, financés ou gérés par les pouvoirs publics. En ce qui concerne les mécanismes flexibles et informels de RAL conçus pour le monde en ligne, aucun pays membre n'a signalé l'existence de dispositions juridiques spécifiques, même si la plupart ont marqué leur intérêt pour la promotion de mécanismes équitables et efficaces de RAL en ligne pour le règlement des petits litiges dans le commerce entreprises-consommateurs, notamment les litiges transfrontières. S'agissant plus spécifiquement du

contexte transfrontière, des différences entre pays ont été notées concernant la validité des contrats à soumettre au RAL, les principes de procédure à utiliser pendant un RAL, la confidentialité et la sécurité des procédures, la validité des accords conclus à l'issue d'un RAL et l'existence ou l'absence de mécanismes de contrainte.

Le volet pédagogique du programme visait à informer l'ensemble des utilisateurs individuels et des entreprises, notamment les petites et moyennes entreprises (PME), de l'existence du RAL et des avantages qui peuvent s'y attacher. Une première série de questions a été établie pour aider les utilisateurs individuels à déterminer si le RAL en ligne pouvait leur permettre de régler un litige, en insistant notamment sur : les points à éclaircir avant d'envisager une procédure de RAL, les considérations entrant dans le choix d'une forme ou une autre de RAL, les moyens permettant de trouver des fournisseurs de services de RAL et les solutions envisageables si le RAL n'est d'aucune aide[10]. Une deuxième série de questions destinée à guider les PME est en préparation.

Enfin, l'OCDE a contribué à la production d'autres informations concernant la disponibilité du RAL en aidant la CCI à établir un inventaire des programmes de RAL à l'échelle mondiale. Le rapport et l'inventaire ainsi établis sont disponibles sur le site Web de la CCI[11].

Mécanismes de respect et de mise en œuvre

Considérant d'une part que plus les décisions sont respectées, moins il est nécessaire de sanctionner, et d'autre part que des systèmes de sanction étoffés peuvent inciter les acteurs à un meilleur respect des décisions, les pays membres de l'OCDE ont entrepris de recenser et d'analyser les mécanismes de sanction qui sont disponibles pour remédier au non-respect des principes et politiques en matière de vie privée et assurer l'accès à des voies de recours[12]. L'objectif était de recueillir, au moyen d'un questionnaire adressé aux pays membres et au secteur privé, des informations qui : *i)* permettraient de mieux comprendre comment les mesures de protection de la vie privée, les mécanismes de sanction, et les moyens de recours possibles peuvent contribuer à mieux protéger la vie privée, comme indiqué dans les Lignes directrices de l'OCDE sur la vie privée et dans la Déclaration ministérielle d'Ottawa ; et *ii)* fourniraient un point de départ pour évaluer l'application concrète des instruments disponibles de mise en application et de sanction dans un environnement de réseaux et leur capacité à répondre aux objectifs des Lignes directrices de l'OCDE sur la vie privée, notamment en termes d'efficacité et de portée interjuridictionnelle.

La synthèse et l'analyse des réponses au questionnaire[13] ont montré que le paysage juridique concernant le respect et la mise en œuvre en matière de vie privée avait changé : si la réglementation par les pouvoirs publics reste le fondement sur lequel repose la confiance des utilisateurs dans le domaine de la vie privée, la réglementation est de plus en plus assortie de mécanismes techniques, organisationnels et d'autorégulation complémentaires pour obtenir une efficacité maximale. Il a été noté qu'un grand nombre d'initiatives de ce type sont en cours dans de nombreux pays membres et que tout montre que leur utilisation se développera rapidement dans les années à venir. De plus, le rapport a mis en lumière le fait que les efforts déployés pour assurer dès le départ le respect de la vie privée représentent une charge moins importante que le besoin d'avoir recours à des mesures de coercition. Il a également démontré qu'il est capital de considérer la protection de la vie privée d'un point de vue mondial, plutôt que purement national, de manière à faciliter les recours contre les violations de la vie privée qui ont un caractère transfrontière.

S'agissant des moyens complémentaires qui permettent de mieux assurer le respect des mesures de protection de la vie privée et leur mise en œuvre, le rapport a montré que les pays membres de l'OCDE et les entités du secteur privé ont développé et continuent de développer des méthodes visant

à : utiliser des incitations et sanctions fondées sur les mécanismes de marché pour assurer le respect des normes ; utiliser des moyens techniques pour mieux garantir leur respect (par exemple technologies protectrices de la vie privée ou audits en ligne) ; offrir des garanties assurées par des tiers ou au niveau de l'entreprise (par exemple programmes de marques de confiance, sceaux, responsables chargés de la protection de la vie privée dans l'entreprise ou politiques de protection de la vie privée en ligne) ; adapter à l'environnement en ligne les mécanismes existants destinés à assurer le respect des mesures de protection de la vie privée et leur mise en œuvre (par exemple possibilité de dépôt de plainte en ligne et RAL pour les litiges liés à la protection de la vie privée) ; et promouvoir des normes techniques, audits, politiques de sécurité et autres mécanismes propres à assurer une meilleure sécurité du traitement des données en ligne.

4) Promouvoir l'éducation et la sensibilisation des utilisateurs à la protection de la vie privée en ligne et aux moyens de protéger la vie privée

Promouvoir l'éducation et les compétences des utilisateurs à l'égard des problèmes de protection de la vie privée en ligne a été l'un des objectifs des travaux de l'OCDE dans tous les domaines, et notamment lors de la conception du Générateur et de l'étude des technologies protectrices de la vie privée. A ce propos, il a été noté que l'éducation et la communication sur la protection de la vie privée en ligne peuvent devoir être adaptées aux besoins des différents participants étant donné la diversité des contraintes, des contextes institutionnels, des hypothèses de base et des perspectives des organisations et des utilisateurs individuels. Les différences culturelles doivent être prises en compte dans la formulation des stratégies visant à améliorer la protection de la vie privée au plan international, que ce soit via le RAL, par l'utilisation de technologies protectrices de la vie privée ou par le recours à toute autre mesure.

5) Encourager l'utilisation de technologies protectrices de la vie privée

Les technologies protectrices de la vie privée sont des outils susceptibles de faciliter la mise en œuvre des principes de protection de la vie privée, tels qu'énoncés dans les Lignes directrices de l'OCDE sur la vie privée, dans le cadre soit d'une autorégulation par l'industrie, soit de réglementations juridiques, soit d'une combinaison de ces approches. Ces technologies peuvent donner aux personnes les moyens de décider elles-mêmes et de contrôler leurs propres données à caractère personnel, mais elles ne permettent pas toutes de la même façon de répondre aux différents problèmes de protection de la vie privée. Des progrès significatifs sont constamment réalisés dans le développement et l'utilisation de ces technologies[14].

Les travaux sur les technologies protectrices de la vie privée ont consisté notamment à dresser un inventaire de ces technologies et à organiser une session spéciale en forum.

L'inventaire des technologies protectrices de la vie privée[15] a été établi pour analyser la disponibilité et la diversité des technologies protectrices de la vie privée, examiner les facteurs qui influent sur l'adoption de ces technologies, analyser la relation entre technologie et vie privée et donner aux décideurs une base à partir de laquelle ils peuvent débattre de l'utilisation et du développement de ces technologies. Ce document[16] a analysé les méthodes de recueil de données à caractère personnel en ligne, examiné différents types de technologies protectrices de la vie privée et formulé des recommandations à l'intention du secteur privé pour encourager le développement et une plus large utilisation de ces technologies. Ces dernières, qui sont des outils techniques susceptibles d'aider à protéger la vie privée en ligne, présentent diverses caractéristiques. Certaines filtrent les « cookies » et les autres technologies de « pistage » ; certaines permettent la consultation du Web et la

pratique du courrier électronique de façon « anonyme » ; d'autres assurent une protection en chiffrant les données ; d'autres encore mettent l'accent sur la protection de la vie privée et la sécurité dans les achats de commerce électronique ; d'autres enfin permettent une gestion évoluée et automatisée des données individuelles des utilisateurs, pour le compte de ces derniers. En substance, les technologies protectrices de la vie privée renforcent la transparence et le choix, ce qui donne aux individus une meilleure maîtrise de la protection de leurs données. Toutefois, nombre de ces technologies peuvent être utilisées de plusieurs façons. Différents produits, technologies et fonctions peuvent répondre à des finalités différentes, selon les préférences de l'utilisateur et la façon dont est mise en œuvre la technologie considérée.

Une session en forum spéciale sur les technologies protectrices de la vie privée[17] a eu lieu à l'OCDE en octobre 2001 pour faciliter les échanges de vues concernant : *i)* les répercussions des technologies protectrices de la vie privée au niveau des politiques ; *ii)* l'avenir des technologies protectrices de la vie privée dans le contexte plus général de la protection de la vie privée en ligne ; et *iii)* les enjeux et les méthodes pour sensibiliser les entreprises à l'importance de la prise en compte de la protection de la vie privée dès la conception des systèmes et de l'utilisation des technologies protectrices de la vie privée, ainsi que pour sensibiliser les individus aux avantages et aux limitations de ces technologies. Cette session a fait clairement ressortir en particulier que sur le plan technique, les technologies protectrices de la vie privée n'offrent pas tout l'éventail des fonctions qui permettraient d'assurer une protection totale de la vie privée, conformément aux Lignes directrices de l'OCDE sur la vie privée [ainsi, parmi les technologies examinées (voir le paragraphe ci-après), un seul outil prend en compte cinq des huit principes de protection de la vie privée, et 58 ne s'appliquent qu'à un seul principe].

Une étude et un document de recherche[18] comprenaient la synthèse d'une étude des technologies protectrices de la vie privée disponibles sur le Web et un tableau des technologies répertoriées, ainsi qu'une discussion de la question de savoir quand, pour qui et dans quelles circonstances une « communication » sur les technologies protectrices de la vie privée pourrait avoir pour résultat d'encourager les entreprises à fournir ces outils et inciter les personnes à les utiliser.

Les technologies protectrices de la vie privée ont été reconnues comme des outils techniques utiles, qui peuvent aider à protéger la vie privée en ligne dans le cadre d'un ensemble plus large d'initiatives de protection de la vie privée en ligne[19]. Elles peuvent donner des moyens d'agir aux utilisateurs individuels qui souhaitent maîtriser la divulgation, l'utilisation et la distribution d'informations de caractère personnel en ligne. Les technologies protectrices de la vie privée peuvent également aider les entreprises et les organisations à mettre en application leurs propres politiques et pratiques en matière de vie privée, et de façon plus générale, à une époque où les utilisateurs individuels sont préoccupés par les questions de vie privée en ligne, elles sont des outils cruciaux pour gérer les flux d'informations à caractère personnel sur les réseaux mondiaux.

Le besoin d'encourager tant les utilisateurs individuels que les entreprises à mettre en place et utiliser ces technologies, a été souligné. Pour que celles-ci soient toutefois plus largement déployées et utilisées, il est apparu qu'elles devraient être d'un usage plus commode, s'accompagner d'informations techniques plus claires et être encore perfectionnées pour couvrir à l'avenir un éventail plus large d'aspects de la protection de la vie privée.

Les premières phases de tout développement technologique étant les plus cruciales, la notion d'intégration des aspects et fonctions de protection de la vie privée dans les solutions techniques a également reçu un accueil favorable. Elle implique pour les développeurs de prendre en compte et d'intégrer les protections en matière de vie privée au moment de la conception et du développement

des systèmes, et pour les entreprises d'examiner dès le départ les répercussions au plan de la vie privée des technologies et services qu'elles mettent en place.

Enfin, l'éducation et la sensibilisation aux technologies protectrices de la vie privée ont été jugées absolument indispensables pour encourager le déploiement et l'utilisation de ces technologies dans les foyers et sur le marché mondial. A cet égard, il a été noté que s'agissant des entreprises et autres organisations, le problème était de les persuader d'internaliser certains coûts (investir dans les technologies protectrices de la vie privée) sur un marché où elles redoutent que leurs concurrents puissent les externaliser. Pour les utilisateurs individuels, il a été noté que le problème de la persuasion dépendait premièrement du degré de préoccupation des différentes catégories de consommateurs quant aux risques pour leur vie privée, et de la nature des risques qui les préoccupaient le plus, et deuxièmement, de la façon dont les préférences individuelles en matière de protection contre divers types de risques font l'objet d'un arbitrage par rapport aux hausses de prix, et troisièmement de la façon dont les individus arbitreront leurs préférences en matière de vie privée par rapport aux coûts de la recherche et du choix d'un autre fournisseur.

6) Encourager l'utilisation et le développement de solutions contractuelles pour les flux transfrontières de données en ligne

Les Lignes directrices de 1980 sur la vie privée stipulent notamment, concernant les flux transfrontières de données :

> « **Partie trois – Principes fondamentaux applicables au plan international : libre circulation et restrictions légitimes**
>
> 15. Les pays membres devraient prendre en considération les conséquences pour d'autres pays membres d'un traitement effectué sur leur propre territoire et de la réexportation des données à caractère personnel.
>
> 16. Les pays membres devraient prendre toutes les mesures raisonnables et appropriées pour assurer que les flux transfrontières de données à caractère personnel, et notamment le transit par un pays membre, ait lieu sans interruption et en toute sécurité.
>
> 17. Un pays membre devrait s'abstenir de limiter les flux transfrontières de données à caractère personnel entre son territoire et celui d'un autre pays membre, sauf lorsque ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays membre peut également imposer des restrictions à l'égard de certaines catégories de données à caractère personnel pour lesquelles sa législation interne pour la protection de la vie privée et de 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.
>
> 18. Les pays membres devraient éviter d'élaborer des lois, des politiques et des procédures qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données à caractère personnel qui iraient au-delà des exigences propres à cette protection. »

Pour contribuer à la solution des problèmes liés aux transactions transfrontières, les pays membres de l'OCDE ont préparé un rapport sur les contrats régissant les flux transfrontières de données dans le cadre des réseaux mondiaux[20]. Ce rapport[21] qui visait pour partie les transactions en ligne d'entreprise à entreprise devrait être lu en parallèle avec d'autres documents plus récents, tels que les contrats-types publiés par la Commission européenne, le Conseil de l'Europe et la Chambre de commerce internationale[22].

L'efficacité des solutions contractuelles a été relevée. Mais le rapport à également mis en lumière le besoin de régler efficacement la question du recours des individus dans les contrats d'entreprise à entreprise relatifs à des flux transfrontières de données et a noté à cet égard que la mise en œuvre de mesures complémentaires, comme la notification des personnes au moment de la collecte des données, est importante.

En ce qui concerne les contrats entre entreprises et consommateurs, le rapport a noté que les tentatives pour élaborer dans un cadre contractuel, des mesures de protection de la vie privée lors des transactions entreprises-consommateurs en ligne posaient problème, notamment lorsqu'il s'agissait de prouver la volonté d'une personne consultant un site Web de se lier par contrat au maître des fichiers de ce site Web, ou lorsqu'une personne souhaite obtenir réparation en vertu d'un contrat. Les pays membres sont donc convenus de se concentrer moins sur les solutions contractuelles et davantage sur une exploration de la façon d'assurer des voies de recours via des mesures de règlement alternatif des litiges en ligne.

NOTES

1. Voir le chapitre 6.
2. Voir le chapitre 7. Le Générateur est disponible à l'adresse : www.oecd.org/sti/security-privacy, ou http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.
3. En juin 2001, Visa international a obligé ses vendeurs en ligne à poster des déclarations de politique en matière de vie privée et les a encouragés à utiliser pour cela le Générateur de l'OCDE. Voir http://international.visa.com/fb/merchants/news/.
4. L'enquête a montré que 75 % des personnes qui avaient vu une déclaration de politique en matière de vie privée en ligne considéraient les déclarations expliquant comment les informations à caractère personnel seront utilisées comme soit « absolument essentielles » soit « très importantes » (Business Week/Harris, mars 2000).
5. Jupiter Research (2002), « Online Privacy : Managing Complexity to Realize Marketing Benefits », 17 mai.
6. L'enquête *Privacy Online : a Report on the Information Practices and Policies of Commercial Websites* publiée en mars 2002 par la *Progress and Freedom Foundation* a porté sur plus de 5 500 sites Web et sur 100 des sites les plus fréquentés.
7. Travaux réalisés en coopération étroite avec le Comité de la politique à l'égard des consommateurs (CPC) de l'OCDE.

8. Voir le chapitre 8.

9. Voir le chapitre 9.

10. Voir le chapitre 10.

11. Voir « Alternative Dispute Resolution Providers : A Global Inventory », juillet 2002 www.iccwbo.org/home/news_archives/2002/stories/adr.asp.

12. Voir le chapitre 11.

13. Projet préparé par un consultant auprès de l'OCDE, M. Chris Kuner, Associé du Cabinet Hunton & Williams.

14. Voir l'Atelier de l'US Department of Commerce (septembre 2000) : www.ntia.doc.gov/ntiahome/privacy.

15. Projet de rapport préparé par une consultante auprès de l'OCDE, Mme Lauren Hall, Directeur, Technology Policy, Advanced Strategy and Policies, Microsoft Corporation, ancienne Executive Vice Président de la Software & Information Industry Association.

16. Voir le chapitre 12.

17. Voir le chapitre 13.

18. Projets préparés par deux consultants auprès de l'OCDE : Laurent Bernat, Responsable de l'information et de la stratégie, Projetweb, et Perri 6, Directeur, The Policy Programme, Institute for Applied Health and Social Policy, King's College, Londres.

19. Cet ensemble plus large comprend l'élaboration et la notification de politiques de protection de la vie privée, le recours à des solutions contractuelles et la disponibilité croissante de mécanismes de recours en ligne – outre les technologies protectrices de la vie privée.

20. Un premier projet de rapport a été établi par une consultante auprès de l'OCDE, Mme Elisabeth Longworth, Sector Director for Information and Communication Technologies, Industry New Zealand, ancienne associée de Longworth Associates.

21. Voir le chapitre 14.

22. Voir les contrats-types de la Commission européenne relatifs aux transferts de données aussi bien pour les transferts de maître de fichier à maître de fichier [Décision de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la Directive 95/46/CE (2001), JO L181/19] et pour les transferts de maître de fichier à sous-traitant [Décision de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la Directive 95/46/CE, (2002), JO L6/52].

    La version finale des clauses de la CCI, soumise à la Commission européenne le 9 août 2002 est disponible à l'adresse : www.iccwbo.org/home/electronic_commerce/word_documents/Final%20version_%20July%202002%20Model%20contract%20clauses.pdf.

    Voir le Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données et son Rapport explicatif, réalisé par le Conseil de l'Europe, la Commission européenne et la Chambre de Commerce Internationale, en date du 2 novembre 1992.

Partie II

POURSUIVRE L'ACTION EN FAVEUR DE LA PROTECTION DE LA VIE PRIVÉE EN LIGNE : ORIENTATIONS POLITIQUES ET PRATIQUES

Chapitre 3

POURSUIVRE L'ACTION EN FAVEUR DE LA PROTECTION DE LA VIE PRIVÉE EN LIGNE : ORIENTATIONS POLITIQUES ET PRATIQUES

Les pays membres de l'OCDE ont pris un engagement collectif, réaffirmé par les Ministres de l'OCDE en 1998, « à l'égard de la protection de la vie privée afin d'assurer le respect de droits importants, de construire la confiance dans l'environnement en ligne et d'empêcher des restrictions inutiles aux flux transfrontières de données à caractère personnel ».

Les orientations politiques et pratiques proposées ci-après répondent à l'objectif principal de la réunion Ministérielle de 1998 visant à établir des passerelles entre les différentes approches adoptées par les pays membres. Elles s'appuient sur les travaux présentés dans la partie I.

Chapitre 3

POURSUIVRE L'ACTION EN FAVEUR DE LA PROTECTION DE LA VIE PRIVÉE EN LIGNE : ORIENTATIONS POLITIQUES ET PRATIQUES

Combiner les approches

Bien que de nombreux systèmes soient des formules hybrides combinant l'autorégulation et l'action législative, la protection de la vie privée a traditionnellement fait l'objet de deux approches : la réglementation gouvernementale et les actions législatives d'une part, et les initiatives d'autorégulation par le marché, d'autre part. Au début de 1998[1], les pays membres de l'OCDE sont convenus que chacune de ces approches présentait des avantages et des inconvénients. Les efforts gouvernementaux semblaient offrir des protections juridiques et des mécanismes de recours prévisibles et contraignants, tandis que les efforts d'autorégulation semblaient donner aux organisations de différents secteurs la possibilité d'adapter des principes directeurs détaillés pour qu'ils fonctionnent dans des contextes spécifiques. Mais ces deux approches laissaient l'une comme l'autre entrevoir des difficultés pour prendre en compte dans des conditions satisfaisantes les questions de vie privée en ligne, notamment dans un cadre transfrontière. Le débat s'est alors déplacé sur le terrain de la panoplie des instruments et techniques qui serait la mieux adaptée pour protéger la vie privée dans l'environnement en ligne mondial.

De fait, les travaux de l'OCDE, on l'a dit, donnent à penser que la meilleure protection de la vie privée en ligne peut, selon toute vraisemblance, être assurée par un éventail d'approches réglementaires et d'autorégulation combinant des solutions juridiques, techniques et pédagogiques adaptées au contexte juridique, culturel et social dans lequel elles opèrent. Tous les instruments, mécanismes, procédures et technologies sont susceptibles de contribuer à renforcer mutuellement leur efficience et leur combinaison permet d'espérer des solutions qui, dépassant l'objectif consistant à établir des passerelles, produiront des solutions viables intégrant différents éléments. Les systèmes de réglementation peuvent être rendus plus efficaces par le recours à un large éventail de mesures d'autorégulation pour mettre en œuvre et faire appliquer la législation en ligne. Les systèmes d'autorégulation peuvent aussi être rendus plus efficients s'ils sont assortis d'une réglementation adéquate et si les pouvoirs publics veillent à leur mise en œuvre effective. Cela garantirait par ailleurs un fonctionnement efficace des marchés assurant la protection de la vie privée. Dans tous les cas, les moyens de contrôle sont essentiels, car la conformité aux exigences de l'un ou l'autre système n'est pas automatique.

Les travaux de l'OCDE ont également démontré qu'une participation résolue et complémentaire de tous les acteurs est indispensable à la mise en œuvre efficace d'une panoplie de mesures de protection de la vie privée, car l'environnement en ligne rend difficile l'application des politiques nationales traditionnelles. Tous les participants ont un rôle à jouer pour contribuer à assurer le respect de la vie privée sur les réseaux mondiaux.

Renforcer la coopération

Compte tenu des travaux déjà accomplis et de ce qu'il reste encore à faire pour aider à assurer une protection efficace de la vie privée au niveau tant national que mondial, il est important que les pays membres de l'OCDE continuent de coopérer entre eux et avec d'autres participants et intensifient leurs efforts pour promouvoir une protection efficace de la vie privée en ligne. A cet égard, des initiatives conjointes appropriées des secteurs public et privé pourraient constituer des stimulants efficaces dans des domaines où les outils technologiques et juridiques sont étroitement interdépendants. De façon plus générale, la poursuite d'efforts cohérents et efficaces pour la protection de la vie privée en ligne à l'intérieur d'un cadre d'action mondial approprié devrait à la fois renforcer la confiance des utilisateurs individuels dans le commerce électronique et plus généralement dans l'environnement en ligne, et permettre aux entreprises et autres organisations de recueillir les bénéfices indirectes de la confiance accrue des consommateurs et utilisateurs individuels.

En conséquence, les pays membres, les entreprises et autres organisations de même que les utilisateurs et consommateurs sont invités à appliquer et faire connaître les orientations politiques et pratiques suivantes, et les pays non membres sont également invités à les prendre en considération.

ORIENTATIONS PRATIQUES POUR LES POLITIQUES DES PAYS MEMBRES DE L'OCDE

Au niveau national

Les pays membres de l'OCDE sont encouragés à continuer de promouvoir efficacement la protection de la vie privée en ligne et de faciliter les échanges et la coopération avec les entreprises et les représentants des utilisateurs et consommateurs, pour définir des mesures et pratiques qui reflètent les orientations politiques et pratiques ci-après. Les pays membres devraient notamment prendre des mesures supplémentaires pour contribuer à assurer :

1) L'adoption de politiques à l'égard de la vie privée, en :

Encourageant les organisations ayant une présence en ligne à :

- Procéder systématiquement à un examen approfondi de leurs pratiques en matière de vie privée et à élaborer une politique mettant en œuvre les principes de l'OCDE en matière de vie privée.
- Examiner les lois et dispositifs d'autorégulation qui peuvent s'appliquer à la collecte de données à caractère personnel et à l'utilisation qu'elles en font, examiner leurs pratiques à la lumière de ces réglementations et les modifier le cas échéant pour mieux respecter leur mise en œuvre.
- Réévaluer de façon régulière leurs pratiques et leur politique en matière de vie privée.
- Utiliser le Générateur de déclaration de politique de protection de la vie privée de l'OCDE[2].

Continuant de promouvoir l'utilisation du Générateur de déclaration de politique de protection de la vie privée de l'OCDE, en tant qu'outil pédagogique et pratique. A cet effet :

- Prendre des initiatives pour créer des hyperliens depuis les sites Web nationaux, vers le site Web de l'OCDE.

- Traduire le Générateur dans leur langue.
- Utiliser le code source[3] pour faire fonctionner le Générateur dans leur propre langue et/ou l'enrichir en y ajoutant une section sur les exigences nationales complémentaires en matière de vie privée.

2) La notification en ligne des politiques en matière de vie privée aux utilisateurs, en :

Encourageant les organisations ayant une présence en ligne **:**

- A afficher en ligne et de façon visible leur politique à l'égard de la vie privée.
- A procéder à des vérifications régulières de la véracité de ces politiques et de leur conformité au droit.

3) La disponibilité de mécanismes de sanction et de recours en cas de non-respect des principes et politiques concernant la vie privée, en :

Encourageant le développement et l'utilisation de mécanismes alternatifs de résolution en ligne des litiges qui soient équitables et efficaces afin de faciliter le règlement des litiges en matière de vie privée ou de consommation, et à cet effet :

- Encourager l'élaboration et la mise à disposition de mécanismes alternatifs de règlement des litiges en ligne flexibles et informels qui tiennent compte du caractère mondial du commerce électronique (par exemple fonctionnement dans plusieurs langues) et permettent de résoudre les litiges transfrontières.
- S'efforcer de réduire les différences entre les cadres juridiques nationaux qui seraient de nature à affecter le caractère opératoire des mécanismes alternatifs de règlement des litiges dans le contexte transfrontière.
- Continuer de fournir des conseils aux utilisateurs sur la manière dont ils peuvent déposer des plaintes et obtenir réparation en cas d'atteinte portée à leur vie privée, en relation avec des échanges en ligne, et mieux faire connaître les différents programmes de règlement alternatif des litiges en ligne qui sont proposés dans les différents pays et les règles qui régissent leur fonctionnement.

Encourageant activement le respect des politiques et principes en matière de vie privée, et à cet effet :

- Mieux sensibiliser les organisations aux avantages de l'élaboration de pratiques et procédures internes efficaces pour renforcer la confiance des utilisateurs individuels, telles la désignation de responsables internes des questions de vie privée et l'autoévaluation volontaire des pratiques en matière de vie privée, ou l'évaluation par des tiers et/ou l'adhésion à des programmes de marques de confiance.

Encourageant l'adoption de solutions efficaces au niveau mondial afin de faire respecter la protection de la vie privée et sanctionner les manquements. A cet effet :

- Encourager l'adoption de mécanismes d'autorégulation, tels que codes de conduite ou programmes de marques de confiance, capables de fonctionner dans un contexte transfrontière et compatibles avec les Lignes directrices de l'OCDE régissant la protection de la vie privée.

- Encourager la nomination par les organisations de responsables internes des questions de vie privée, en fournissant une base légale à cette fonction et/ou en créant des incitations légales au recours à ce type de fonction par les organisations.
- Continuer de proposer des ressources en ligne pour le traitement des plaintes.
- Renforcer les mécanismes de sanction contre les organisations qui ne représentent pas la réalité en ce qui concerne leur respect des politiques en matière de vie privée et autres types d'engagement pris dans ce domaine vis-à-vis des utilisateurs individuels.

4) Le soutien de l'éducation et de la sensibilisation des utilisateurs aux questions de vie privée et aux moyens de protection de leur vie privée, en :

- Encourageant des actions efficaces d'éducation et d'information en direction des organisations et des utilisateurs individuels relatives aux questions de protection de la vie privée en ligne et aux solutions existantes, y compris les technologies protectrices de la vie privée.
- Continuant de proposer des ressources en ligne pour mieux sensibiliser aux réglementations et pratiques exemplaires en matière de protection de la vie privée.
- Sensibilisant davantage les utilisateurs individuels afin de mieux leur faire comprendre la technologie et les implications pour la vie privée des transactions et échanges sur Internet.
- Soutenant les travaux universitaires visant à analyser plus en détail la façon de persuader efficacement les organisations et les utilisateurs individuels d'avoir recours à une panoplie efficace et complémentaire de solutions de protection de la vie privée en ligne.

5) L'utilisation de technologies protectrices de la vie privée et le développement de fonctions de protection de la vie privée dans d'autres technologies, selon les besoins, en :

- Encourageant activement les développeurs de systèmes et d'applications logicielles à intégrer, dès le stade de la conception, la protection de la vie privée dans les technologies de l'information.
- Encourageant activement les organisations à envisager à un stade précoce les répercussions sur la vie privée des technologies et services qu'elles mettent en œuvre.
- Proposant des incitations, par exemple des actions conjointes appropriées avec le secteur privé, pour continuer à développer un marché durable pour des technologies protectrices de la vie privée conçues pour les utilisateurs individuels et pour les organisations, et en encourageant un plus large recours à ces outils.
- Éduquant et sensibilisant, de façon plus générale, aux solutions techniques, et encourageant les organisations à fournir aux utilisateurs individuels des technologies conviviales et transparentes et, de la même manière, en encourageant les utilisateurs à avoir recours à ces technologies et partant à chercher à s'informer sur les options de protection de la vie privée en ligne et à se former à leur utilisation.

Au niveau mondial

Les pays membres de l'OCDE devraient réaffirmer leur intention de coopérer entre eux et avec les autres participants pour mettre en œuvre en ligne, dans les secteurs public et privé, les Lignes directrices de l'OCDE sur la vie privée. Comme l'ont indiqué les Ministres de l'OCDE dans leur Déclaration de 1998, les pays membres devraient également envisager de réévaluer périodiquement la nécessité d'entreprendre d'autres actions complémentaires pour assurer la protection des données à caractère personnel au niveau mondial.

Les pays membres devraient notamment, dans le contexte de l'environnement en ligne mondial :

- Insister sur l'importance de la partie cinq des Lignes directrices de 1980 régissant la protection de la vie privée[4] qui concerne la coopération internationale, et s'efforcer d'établir des procédures pour améliorer les mécanismes bilatéraux et multilatéraux de coopération transfrontière entre les organismes publics chargés de l'application de la loi et concernés par les aspects de procédure ou d'investigations associés aux Lignes directrices ou prévus par elles.
- Continuer de coordonner leur action avec celle du secteur privé et explorer par quels moyens le recours à des partenariats public/privé pourrait aider à renforcer la confiance des organisations et utilisateurs individuels en ligne dans des domaines où la technologie et la réglementation sont étroitement liées, comme le règlement des litiges en ligne et les technologies protectrices de la vie privée.
- Promouvoir la coopération avec les autres organisations internationales, selon les besoins.
- Continuer d'explorer les moyens de renforcer la confiance en ligne parmi l'ensemble des participants, par des actions appropriées d'ouverture, d'éducation, de coopération et de consultation.

ORIENTATIONS PRATIQUES A L'INTENTION DES ENTREPRISES ET AUTRES ORGANISATIONS

Les entreprises et autres organisations ne doivent pas attendre d'être encouragées par les gouvernements aux niveaux national et international pour continuer de promouvoir et améliorer la protection de la vie privée en ligne. Très souvent, elles peuvent de leur propre initiative appliquer les politiques et orientations pratiques susmentionnées. Elles peuvent notamment :

- Élaborer des politiques en matière de vie privée en s'appuyant sur les Lignes directrices de l'OCDE, utiliser le Générateur de l'OCDE et des mécanismes analogues qui constituent des outils utiles facilitant l'élaboration de politiques, et poster leurs politiques en matière de vie privée sur leur page d'accueil.
- Évaluer si les outils d'autorégulation suivants sont adaptés à leurs activités et dans l'affirmative, les mettre en place et s'y conformer : programmes de marques de confiance ; codes de conduite ; systèmes de labellisation ; icônes ou symboles relatifs à la vie privée ; audits, soit par autoévaluation, soit pas des tiers ; et mécanismes efficaces de recours, notamment en matière de règlement alternatif des litiges.
- Travailler avec les pouvoirs publics pour développer des modèles innovants et souples afin de mettre en œuvre les modèles réglementaires et d'autorégulation existants et naissants, et faire en sorte que les besoins légitimes de flux d'informations soient pris en compte, en même temps que les besoins légitimes de protection des données à caractère personnel.

ORIENTATIONS PRATIQUES À L'INTENTION DES UTILISATEURS INDIVIDUELS ET DES CONSOMMATEURS

Les utilisateurs individuels et les consommateurs peuvent agir directement ou par l'intermédiaire de groupes représentatifs pour protéger leurs intérêts en :

- Demandant l'adoption par les entreprises et autres organisations de pratiques efficaces en matière de vie privée, de politiques claires en la matière et de technologies protectrices de la vie privée, s'ils considèrent qu'elles leur seraient utiles en tant qu'utilisateurs.
- Demandant de façon plus générale davantage de transparence et d'information didactique.
- Faisant valoir leurs droits légaux au regard de la législation nationale, notamment, le cas échéant, leurs droits d'accès et de rectification en cas de manquement.

Les utilisateurs devraient être encouragés par des mesures pédagogiques appropriées à prendre individuellement la responsabilité de la protection de leurs données personnelles, soit par des mesures d'autoprotection (comme l'utilisation de technologies protectrices de la vie privée, la lecture attentive des déclarations de politique de protection de la vie privée et le refus de communiquer leurs données à des tiers, selon le cas) soit par des mesures permettant de résoudre les litiges et d'obtenir un dédommagement (comme le recours à des systèmes de règlement alternatif des litiges et le dépôt de plaintes auprès des organismes compétents).

NOTES

1. Atelier de l'OCDE sur la protection de la vie privée dans une société de réseau mondialisée (février 1998). Voir www.oecd.org/ EN/documents/0,,EN-documents-43-1-no-4-no-43,00.html.

2. Voir le chapitre 7 et http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

3. L'OCDE met les codes sources du Générateur à la disposition des pays membres de l'OCDE afin qu'ils puissent l'intégrer sur leurs sites nationaux et y adjoindre les données propres au pays. Le code source peut être communiqué à toute organisation des pays membres qui remplit une mission officielle pour son propre usage. Le code source ne peut toutefois être distribué aux entreprises privées poursuivant une activité commerciale ou lucrative.

4. PARTIE CINQ : COOPERATION INTERNATIONALE

« 20. Les pays membres devraient, sur demande, faire connaître à d'autres pays membres les modalités détaillées de l'application des principes énoncés dans les présentes Lignes directrices. Les pays membres devraient également veiller à ce que les procédures applicables aux flux transfrontières de données de caractère personnel, ainsi qu'à la protection de la vie privée et des libertés individuelles soient simples et compatibles avec celles des autres pays membres qui se conforment aux présentes Lignes directrices.

21. Les pays membres devraient établir des procédures en vue de faciliter :

- l'échange d'informations relatives aux présentes Lignes directrices ; et

- l'assistance mutuelle lorsqu'il s'agit des questions de procédures et d'échange réciproque d'information.

22. Les pays membres devraient s'employer à établir des principes, au plan intérieur et international, afin de déterminer le droit applicable en cas de flux transfrontières de données de caractère personnel. »

Partie III

DOCUMENTS DE RÉFÉRENCE

Chapitre 4

LES LIGNES DIRECTRICES RÉGISSANT LA PROTECTION DE LA VIE PRIVÉE ET LES FLUX TRANSFRONTIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

Le Conseil de l'OCDE a adopté en tant que Recommandation, les Lignes directrices régissant la protection de données à caractère personnel comme mesure de soutien des trios principes qui tient les pays membres de l'OCDE : la démocratie plurielle, le respect des droits humains et une économie de marché ouverte. Elles sont entrées en vigueur le 23 septembre 1980.

LES LIGNES DIRECTRICES RÉGISSANT LA PROTECTION DE LA VIE PRIVÉE ET LES FLUX TRANSFRONTIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

RECOMMANDATION DU CONSEIL CONCERNANT LES LIGNES DIRECTRICES RÉGISSANT LA PROTECTION DE LA VIE PRIVÉE ET LES FLUX TRANSFRONTIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

(23 septembre 1980)

LE CONSEIL,

Vu les Articles 1 *(c),* 3 *(a)* et 5 *(b)* de la Convention relative à l'Organisation de Coopération et de Développement Économiques en date du 14 décembre 1960 ;

RECONNAISSANT :

que, bien que les législations et politiques nationales puissent différer, il est de l'intérêt commun des pays Membres de protéger la vie privée et les libertés individuelles et de concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information ;

que le traitement automatique et les flux transfrontières de données de caractère personnel créent de nouvelles formes de relations entre pays et exigent l'instauration de règles et pratiques compatibles ;

que les flux transfrontières de données de caractère personnel contribuent au développement économique et social ;

que les droits internes concernant la protection de la vie privée et les flux transfrontières de données de caractère personnel sont susceptibles d'entraver ces flux transfrontières ;

Résolu à favoriser la libre circulation de l'information entre les pays Membres et à éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre ces pays ;

RECOMMANDE :

1. 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 figurant en Annexe à la présente Recommandation dont elle fait partie intégrante ;
2. Que les pays Membres s'efforcent de supprimer ou d'éviter de créer, au nom de la protection de la vie privée, des obstacles injustifiés aux flux transfrontières des données de caractère personnel ;
3. Que les pays Membres coopèrent pour mettre en œuvre les lignes directrices énoncées en Annexe ;
4. Que les pays Membres conviennent dès que possible de procédures spécifiques de consultation et de coopération en vue de l'application des présentes lignes directrices.

Annexe à la recommandation du conseil du 23 septembre 1980

LIGNES DIRECTRICES RÉGISSANT LA PROTECTION DE LA VIE PRIVÉE ET LES FLUX TRANSFRONTIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

PREMIÈRE PARTIE. CONSIDÉRATIONS GÉNÉRALES

Définitions

1. Aux fins des présentes lignes directrices :

a) par « maître du fichier », on entend toute personne physique ou morale qui, conformément au droit interne, est habilitée à décider du choix et de l'utilisation des données de caractère personnel, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom ;

b) par « données de caractère personnel », on entend toute information relative à une personne physique identifiée ou identifiable (personne concernée) ;

c) par « flux transfrontière de données de caractère personnel », on entend la circulation de données de caractère personnel à travers les frontières nationales.

Champ d'application des lignes directrices

2. Les présentes lignes directrices s'appliquent aux données de caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles.

3. Les présentes lignes directrices ne devraient pas être interprétées comme interdisant :

a) d'appliquer, à diverses catégories de données de caractère personnel, des mesures de protection différentes selon leur nature et le contexte dans lequel elles sont collectées, enregistrées, traitées ou diffusées ;

b) d'en exclure l'application à des données de caractère personnel qui, manifestement, ne présentent aucun risque pour la vie privée et les libertés individuelles, ou

c) d'en limiter l'application au traitement automatique des données de caractère personnel.

4. Les exceptions aux principes énoncés dans les Parties Deux et Trois des présentes lignes directrices, y compris celles intéressant la souveraineté nationale, la sécurité nationale et l'ordre public, devraient être :

a) aussi peu nombreuses que possible, et
b) portées à la connaissance du public.

5. Dans le cas particulier des pays à structure fédérale, l'application des présentes lignes directrices peut être influencée par la répartition des pouvoirs dans l'État fédéral.

6. Les présentes lignes directrices devraient être considérées comme des normes minimales susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et les libertés individuelles.

PARTIE DEUX. PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN NATIONAL

Principe de la limitation en matière de collecte

7. 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.

Principe de la qualité des données

8. 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.

Principe de la spécification des finalités

9. 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.

Principe de la limitation de l'utilisation

10. Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe 9, si ce n'est :

a) avec le consentement de la personne concernée ; ou
b) lorsqu'une règle de droit le permet.

Principe des garanties de sécurité

11. Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.

Principe de la transparence

12. Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

Principe de la participation individuelle

13. Toute personne physique devrait avoir le droit :

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ;

b) de se faire communiquer les données la concernant ;

i) dans un délai raisonnable ;
ii) moyennant, éventuellement, une redevance modérée ;
iii) selon des modalités raisonnables ; et
iv) sous une forme qui lui soit aisément intelligible ;

c) d'être informée des raisons pour lesquelles une demande quelle 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.

Principe de la responsabilité

14. Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

PARTIE TROIS. PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN INTERNATIONAL : LIBRE CIRCULATION ET RESTRICTIONS LÉGITIMES

15. Les pays Membres devraient prendre en considération les conséquences pour d'autres pays Membres d'un traitement effectué sur leur propre territoire et de la réexportation des données de caractère personnel.

16. Les pays Membres devraient prendre toutes les mesures raisonnables et appropriées pour assurer que les flux transfrontières de données de caractère personnel, et notamment le transit par un pays Membre, aient lieu sans interruption et en toute sécurité.

17. Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, sauf lorsqu'un ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de protection équivalente.

18. Les pays Membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-delà des exigences propres à cette protection.

PARTIE QUATRE. MISE EN ŒUVRE DES PRINCIPES A L'ÉCHELON NATIONAL

19. Lors de la mise en œuvre, au plan intérieur, des principes énoncés dans les Parties Deux et Trois, les pays Membres devraient établir des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée et les libertés individuelles eu égard aux données de caractère personnel. Les pays Membres devraient notamment s'efforcer de :

a) adopter une législation nationale appropriée ;
b) favoriser et soutenir des systèmes d'autoréglementation (codes de déontologie ou autres formes) ;
c) permettre aux personnes physiques de disposer de 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 énoncés dans les Parties Deux et Trois ; et
e) veiller à ce que les personnes concernées ne fassent l'objet d'aucune discrimination inéquitable.

PARTIE CINQ. COOPÉRATION INTERNATIONALE

20. Les pays Membres devraient, sur demande, faire connaître à d'autres pays Membres les modalités détaillées de l'application des principes énoncés dans les présentes lignes directrices. Les pays Membres devraient également veiller à ce que les procédures applicables aux flux transfrontières de données de caractère personnel, ainsi qu'à la protection de la vie privée des libertés individuelles, soient simples et compatibles avec celles des autres pays Membres qui se confirment aux présentes lignes directrices.

21. Les pays Membres devraient établir des procédures en vue de faciliter :

i) l'échange d'informations relatives aux présentes lignes directrices ; et
ii) l'assistance mutuelle lorsqu'il s'agit des questions de procédure et d'échange réciproque d'information.

22. Les pays Membres devraient s'employer à établir des principes, au plan intérieur et international, afin de déterminer le droit applicable en cas de flux transfrontières de données de caractère personnel.

Chapitre 5

DÉCLARATION MINISTÉRIELLE RELATIVE À LA PROTECTION DE LA VIE PRIVÉE SUR LES RÉSEAUX MONDIAUX

La déclaration relative à la protection de la vie privée sur les réseaux mondiaux qui a été adoptée par les Ministres à la Conférence « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial » tenue à Ottawa, Canada, 7-9 octobre 1998. A sa 934ème session, le 19 octobre 1998, le Conseil a adopté une Résolution intégrant cette Déclaration dans les instruments de l'Organisation.

Chapitre 5

DÉCLARATION MINISTERIELLE RELATIVE À LA PROTECTION DE LA VIE PRIVÉE SUR LES RÉSEAUX MONDIAUX

Les Gouvernements des pays Membres de l'OCDE[1] :

Considérant que le développement et la diffusion à l'échelle mondiale des technologies numériques de l'informatique et des réseaux présentent des avantages sociaux et économiques en encourageant les échanges d'informations, en élargissant le choix offert aux consommateurs, et en favorisant l'expansion des marchés et l'innovation de produits ;

Considérant que les technologies des réseaux mondiaux facilitent l'expansion du commerce électronique et accélèrent le développement des communications et des transactions électroniques transfrontières entre gouvernements, entreprises, utilisateurs et consommateurs ;

Considérant que le recueil et la manipulation de données de caractère personnel devraient s'effectuer dans le dû respect de la vie privée ;

Considérant que les technologies numériques de l'informatique et des réseaux améliorent les méthodes traditionnelles de traitement des données de caractère personnel, augmentent l'aptitude à collecter, rassembler et rapprocher d'importantes quantités de données et à produire des informations enrichies et des profils de consommateurs ;

Considérant que les technologies numériques de l'informatique et des réseaux peuvent aussi être utilisées pour instruire les utilisateurs et les consommateurs des problèmes de protection de la vie privée en ligne, et pour les aider à préserver leur anonymat dans des circonstances appropriées ou à exercer leur liberté de choix eu égard aux utilisations qui sont faites de leurs données personnelles ;

Considérant que pour accroître la confiance dans les réseaux mondiaux, les utilisateurs et consommateurs ont besoin d'avoir des assurances quant au caractère loyal de la collecte et du traitement des données personnelles les concernant, notamment des données relatives à leurs activités et transactions en ligne ;

Considérant que des mesures sont nécessaires pour assurer la protection efficace et généralisée de la vie privée par les entreprises qui collectent ou traitent des données de caractère personnel, de manière à accroître la confiance des utilisateurs et consommateurs dans les réseaux mondiaux ;

Considérant que des règles et règlements transparents régissant la protection de la vie privée et des données de caractère personnel et leur mise en œuvre efficace sur les réseaux d'information sont un élément clé pour accroître la confiance dans les réseaux mondiaux ;

1. Incluant les Communautés européennes.

Considérant que des approches différentes et efficaces élaborées, en matière de protection de la vie privée, par les pays Membres, notamment l'adoption et la mise en œuvre de lois ou de dispositifs d'autorégulation par l'industrie, peuvent se combiner pour parvenir à un niveau efficace de protection de la vie privée sur les réseaux mondiaux ;

Considérant le besoin de coopération mondiale, et la nécessité que le secteur industriel et commercial joue un rôle majeur, en concertation avec les consommateurs et les pouvoirs publics, pour assurer la mise en œuvre efficace des principes de protection de la vie privée sur les réseaux mondiaux ;

Considérant que les principes technologiquement neutres énoncés dans les Lignes directrices de l'OCDE sur la protection de la vie privée de 1980 continuent de refléter un consensus international sur les orientations qui doivent guider la collecte et la manipulation des données de caractère personnel sur quelque support que ce soit, et fournissent une base sur laquelle fonder la protection de la vie privée sur les réseaux mondiaux ;

RÉAFFIRMENT les objectifs énoncés dans **:**

La Recommandation concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptée par le Conseil de l'OCDE le 23 septembre 1980 (Lignes directrices de l'OCDE sur la protection de la vie privée) ;

La Déclaration sur les flux transfrontières de données, adoptée par les Gouvernements des pays Membres de l'OCDE le 11 avril 1985 ; et

La Recommandation relative aux Lignes directrices régissant la politique de cryptographie, adoptée par le Conseil de l'OCDE le 27 mars 1997.

DÉCLARENT :

Qu'ils vont réaffirmer leur engagement à l'égard de la protection de la vie privée sur les réseaux mondiaux, afin d'assurer le respect de droits importants, de construire la confiance dans les réseaux mondiaux et d'empêcher des restrictions inutiles aux flux transfrontières de données de caractère personnel ;

Qu'ils s'attacheront à établir des passerelles entre les différentes approches adoptées par les pays Membres en vue de garantir la protection de la vie privée sur les réseaux mondiaux sur la base des Lignes directrices de l'OCDE ;

Qu'ils prendront, dans le cadre de leurs lois et pratiques respectives, les mesures nécessaires pour garantir la mise en œuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée en ce qui concerne les réseaux mondiaux, en veillant notamment :

à encourager l'adoption de politiques en matière de vie privée, qu'elles soient mises en œuvre par le recours à des mécanismes juridiques, administratifs, technologiques ou d'autorégulation ;

à encourager la notification en ligne aux utilisateurs des politiques en matière de vie privée ;

à garantir l'existence de mécanismes efficaces de mise en œuvre permettant à la fois de régler les problèmes de non-respect des principes et des politiques de vie privée et de garantir l'accès à des moyens de réparation ;

à promouvoir l'éducation et la sensibilisation des utilisateurs aux problèmes de respect de la vie privée en ligne et aux moyens dont ils disposent pour protéger leur vie privée sur les réseaux mondiaux ;

à encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée ; et

à encourager l'utilisation de solutions contractuelles et le développement de solutions contractuelles types pour les flux transfrontières de données en ligne ;

Qu'ils conviennent de faire le point des progrès accomplis pour se rapprocher des objectifs de la présente Déclaration, dans un délai de deux ans, et d'évaluer la nécessité d'actions supplémentaires pour assurer la protection des données de caractère personnel sur les réseaux mondiaux afin d'atteindre ces objectifs.

DÉCLARENT EN OUTRE QUE L'OCDE DEVRAIT :

Aider les pays Membres à échanger des informations sur les méthodes efficaces pour protéger la vie privée sur les réseaux mondiaux et à faire part de leurs efforts et de leur expérience dans la réalisation des objectifs de la présente Déclaration ;

Examiner les problèmes spécifiques soulevés par la mise en œuvre des Lignes directrices de l'OCDE sur la protection de la vie privée en relation avec les réseaux mondiaux, et, après avoir collecté et diffusé des exemples d'expériences de mise en œuvre les Lignes directrices, fournir aux pays Membres des orientations pratiques pour la mise en œuvre des Lignes directrices dans l'environnement en ligne, en tenant compte des différentes approches à l'égard de la protection de la vie privée adoptées par les pays Membres et en s'inspirant de l'expérience des pays Membres et du secteur privé ;

Coopérer avec l'industrie et les entreprises dans le cadre de leurs travaux en vue d'assurer la protection de la vie privée sur les réseaux mondiaux, ainsi qu'avec les organisations régionales et internationales compétentes ;

Faire périodiquement le point des principales évolutions et questions dans le domaine de la protection de la vie privée eu égard aux objectifs de la présente Déclaration ;

Prendre notamment en considération, dans le cadre de ses travaux futurs, les questions et les suggestions d'activités présentées dans le rapport qui accompagne cette Déclaration.

INVITENT :

Les pays non membres à tenir compte de la présente Déclaration ;

Les organisations internationales compétentes à prendre en considération la présente Déclaration lorsqu'elles élaborent ou modifient des conventions internationales, des Lignes directrices, des codes de conduite, des clauses contractuelles types, des technologies et des plates-formes interopérables pour la protection de la vie privée sur les réseaux mondiaux ;

L'industrie et les entreprises à prendre en compte les objectifs de la présente Déclaration et à collaborer avec les gouvernements pour promouvoir ces objectifs en mettant en œuvre des programmes visant la protection de la vie privée sur les réseaux mondiaux.

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 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 PRIVÉE[1]

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 comprendre[2] :

- 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 Web[5]. 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 oeuvre d'actions répressives.

Dans certains pays membres de l'OCDE, on considère l'autorégulation comme un moyen souple et efficient 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 particulière[6], 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 données[9]. 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 coopération[10] 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 personnel[11]. 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 mondiaux[12].

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 équivalente[16].

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 données[17]. 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 données[18], 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 européenne[20]. 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 manuel[21].

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 sensibles[22], des exigences d'information détaillées[23], des dispositions de notification[24], des droits d'opposition des personnes concernées pour se soustraire aux sollicitations commerciales[25], et de recours[26].

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 privée[27], 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 obtenu[29].

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 justice[30].

Concernant la mise en oeuvre de ses dispositions, la directive de l'Union européenne prévoit des recours juridictionnels, des responsabilités et des sanctions[31]. 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 20ème 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 « Mémorandum 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 privée[39]. 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 concernant[45]. 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 pénaux[46].

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

Le gouvernement fédéral allemand a promulgué un nombre appréciable de lois et règlements[47] 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 données[50]. Les Commissaires à la protection des données de la Fédération et des Länder tiennent régulièrement des conférences[51]. 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 européenne[52]. 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 pénales[57]. 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 Parlement[60].

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 loi[61]. 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 privée[62].

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 belge[63].

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 clients[64].

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'OCDE[66]. Diverses lois sectorielles garantissent la protection de la vie privée dans des domaines comme les informations de santé des personnes[67].

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 1996[69]. 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.

Instruments d'autorégulation

L'Ombudsman pour les questions intéressant les consommateurs élabore actuellement un ensemble de règles déontologiques destinées à être mises en oeuvre 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'infraction[74].

Autres lois comportant des dispositions de protection de la vie privée

Il existe en Espagne une loi sur les statistiques publiques[75] 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'Internet[76]. 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 œuvre 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 Etats-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 réglemente 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 violations[90].

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 1er 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 électronique[91] 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'emprisonnement[94]. 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'Internet[98], 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 78/17[99]. 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 européenne[100]. 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 infractions[101].

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 traitement[102]. La loi prévoit une réparation, par la voie civile, des dommages causés en infraction à la loi[103], des sanctions administratives (telles que des amendes et l'annulation des licences de traitement de données)[104] ainsi que des sanctions pénales[105].

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 Commissaire[108] ou en intentant une action en justice[109].

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 privée[110].

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 autorisée[111]. 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 conduite[112] 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 oeuvre, 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 Loi[113] 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 personnel[114]. Elles peuvent aussi demander que leur nom soit rayé des listes de publipostage[115]. 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 concernées[116].

La loi de 1989 établit des sanctions pénales pour les infractions à certaines dispositions[117].

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'usager, 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. Contenues 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 privé[118].

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 privé[119]. 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 application[120]. 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 dispositions[126].

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 médicaux[127].

Mise en œuvre de la directive de l'Union européenne

Un projet de loi transposant la directive de l'Union européenne a été rédigé[128]. 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 publiques[129].

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.

Instruments 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 publics[131].

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 IPP[133].

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 Politieregisters*, 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 médiales (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 1er 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 persoonsgevens* (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 1er septembre 2001 doit être conforme aux nouvelles dispositions. Une période de transition d'un an, qui s'est terminée le 1er 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 personnel[140].

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 plaintes[144] 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 suppression[145]. Les infractions à la loi[146], 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 humains[148] ou le Centre des cartes d'identité[149], et les réglementations régissant les bases de données exploitées par la Gendarmerie[150], les Services des affaires frontalières et étrangères[151] et la Police criminelle[152].

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 1er 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 1er 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 1er 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 1er 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 données[154]. 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'Homme[161]. 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 données[164].

SUÈDE

Constitution

La Constitution suédoise (loi sur la liberté de la presse[165]) garantit le droit des personnes à accéder aux documents et données détenus par les autorités publiques. De plus, la Constitution[166] 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 personnelles[167] 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 gouvernement[168] 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'auto-régulation.

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 limités[172]. 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 recours[173].

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 suisse[174], 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 gomment 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 collecter[175]. 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 utilisateurs[180], 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'anonymat[182] 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 mondiaux[183]. *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 croître[190]. 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'utilisateur[195]. 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 suivantes[196] : 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 incluse[197]. 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 préférences[200]. 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 réclamations[201].

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 cookie[203]. 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 listes[205]. 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 enregistrées[207].

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 adéquate[208].

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 concernées[209], 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 tiers[210]. Cette révision prend en compte les commentaires du groupe de travail de la Commission européenne établi conformément à l'article 29 de la directive[211].

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 privée[212].

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 données[213] 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 continûment à ces contrôles affichent une marque de certification, comme un label numérique[214] ou une icône

reconnue[215], 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'autorégulation[216] 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 « ensemençant » 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-comptables[218]. 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 certification[219]. 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 Etats-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 Etats-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 qualificatifs, éventuellement en établissant une charte distincte pour la protection de la vie privée représentée par un label ou une icône spécifique[222].

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 européenne[223], 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 autorités[224], 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 Web[225].

- L'exclusion de l'association professionnelle[226] ; 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 intenter 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 trompeuses[228]. 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 loi[229]. 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 consentement[230]. 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 graves[231]. 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'application[232].

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'Europe[234] ; *ii)* des organismes gouvernementaux, comme la FTC aux Etats-Unis[235], beaucoup d'autorités centrales de surveillance dans d'autres parties du monde[236] 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 TRUSTe[240]. 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'il 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 1er 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 *Datenshutzkommission* 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.cbpweb.nl.

139. Wet van 19 oktober 1998, Stb.610, houdende regels inzake de telecommunicatie (Telecommmunicatiewet).

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 gouvernmentaux, 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 23ème 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 Etats 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/brfovrvw.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 ? », 18ème 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-compcon97-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.

Chapitre 7

LE GÉNÉRATEUR DE DÉCLARATION DE PROTECTION DE LA VIE PRIVÉE DE L'OCDE

Ce chapitre présente les principales pages de le Générateur de déclaration de protection de la vie privée de l'OCDE, un outil gratuit fourni en ligne sur l'Internet et disponible à : http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

QU'EST-CE QUE LE GÉNÉRATEUR DE DÉCLARATION DE PROTECTION DE LA VIE PRIVÉE DE L'OCDE ?

POURQUOI ÉLABORER UNE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE ET POURQUOI L'AFFICHER DANS UNE DÉCLARATION ?

La recherche relative à l'Internet a maintes fois démontré que de nombreux consommateurs hésitent à effectuer des transactions électroniques parce qu'ils craignent que cela ne porte atteinte à la confidentialité de leurs données à caractère personnel. Des politiques de protection de la vie privée et des déclarations publiques affichant ces politiques représentent une étape indispensable pour encourager la transparence et inciter les visiteurs aux sites Web à avoir confiance dans le commerce électronique. Elles peuvent aider les visiteurs à faire des choix éclairés lorsqu'il s'agit de confier des **données à caractère personnel** à une organisation et de s'engager dans des transactions commerciales.

CADRE GÉNÉRAL DU GÉNÉRATEUR DE L'OCDE

Les **Lignes directrices de l'OCDE sur la protection de la vie privée** traduisent le consensus international qui s'est dégagé sur la meilleure façon de concilier une protection efficace de la vie privée avec la libre circulation des **données personnelles**. La **transparence** est un principe clé de ces Lignes directrices qui sont souples et auxquelles on peut se conformer de diverses façons.

Afin d'encourager la mise en œuvre des Lignes directrices dans le monde électronique, l'OCDE a élaboré le Générateur de déclaration de politique de protection de la vie privée de l'OCDE en collaboration avec **l'industrie, les spécialistes de la protection de la vie privée et les associations de consommateurs**. Le Générateur, que les **30 pays Membres de l'OCDE** ont approuvé, a pour objet de fournir des indications sur la mise en conformité avec les Lignes directrices et d'aider les organisations à développer des politiques de protection de la vie privée et des déclarations s'y rattachant qui seront affichées sur leurs sites Web.

En mettant le Générateur en ligne gratuitement, on espère qu'il aidera à :

- Sensibiliser davantage les propriétaires de sites.
- Permettre aux visiteurs de mieux appréhender les pratiques en matière de protection de la vie privée qui ont cours sur les sites où ils naviguent.
- Encourager la confiance des utilisateurs et des consommateurs dans les réseaux mondiaux et le commerce électronique.

Toutefois, l'emploi du Générateur de l'OCDE n'implique pas nécessairement que le site Web se conforme aux Lignes directrices de l'OCDE sur la protection de la vie privée.

QU'EST-CE QUE LE GÉNÉRATEUR DE DÉCLARATION DE PROTECTION DE LA VIE PRIVÉE DE L'OCDE ?

Le Générateur est avant tout un outil éducatif.

Il fournit des conseils pour procéder, à l'intérieur de l'organisation, à l'examen des pratiques en matière de protection de la vie privée, et pour élaborer une déclaration de politique de protection de la vie privée. Il fournit des liens vers les organisations du secteur privé possédant une expertise en matière d'élaboration de politiques de protection de la vie privée, de même que vers des agences gouvernementales, des organisations non gouvernementales et des entités du secteur privé qui fournissent des informations sur les règlements applicables.

Pour vous informer sur vos pratiques en matière de protection de la vie privée, le Générateur utilise un questionnaire. La section intitulée « Aide » fournit des notes explicatives et des conseils pratiques. Dans certains cas, on attire votre attention au moyen d'avertissements. Vos réponses sont ensuite incorporées dans un projet de déclaration de politique préformaté. Vous devez évaluer cette déclaration : reflète-t-elle fidèlement vos pratiques et votre politique en matière de données à caractère personnel ?

Veuillez noter que l'OCDE ne garantit pas que ce projet de déclaration de politique de protection de la vie privée réponde aux prescriptions légales ou aux dispositifs d'autorégulation applicables. La déclaration reflète simplement les réponses fournies aux questions du Générateur. Le projet de déclaration permettra toutefois d'évaluer la conformité de vos pratiques avec les **Lignes directrices de l'OCDE sur la protection de la vie privée**.

LIMITES ET CONDITIONS D'UTILISATION DU GÉNÉRATEUR DE DÉCLARATION DE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE

Le Générateur est mis gratuitement à la disposition de toute organisation privée ou publique sur le site Web de l'OCDE. Si vous trouvez le Générateur sur le site Web d'une agence gouvernementale ou d'une entité similaire, il pourrait contenir une section supplémentaire destinée à aider à la mise en conformité avec les exigences spécifiques de ce pays.

L'OCDE a élaboré le Générateur de l'OCDE pour aider au développement d'une politique de protection de la vie privée et à l'élaboration de la déclaration qui s'y rattache.

On s'attend à ce que les utilisateurs agissent loyalement et en toute bonne foi vis-à-vis du Générateur et de la substance des déclarations qu'il produit.

L'utilisation du Générateur n'implique pas et ne doit pas impliquer que l'OCDE autorise ou donne son aval à la politique de protection de la vie privée ou à la déclaration élaborée par les utilisateurs. Ceux-ci peuvent toutefois indiquer qu'ils se sont servis du Générateur de l'OCDE pour l'élaboration de leur politique de protection de la vie privée et de la déclaration qui s'y rattache. Dans ce cas ils devraient fournir un lien à http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

- □ Lire d'abord **Élaboration d'une politique de protection de la vie privée**
- □ Commencer le **questionnaire**

ÉLABORATION D'UNE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE ET D'UNE DÉCLARATION S'Y RATTACHANT

COMMENT DÉVELOPPER UNE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE

1ÈRE ÉTAPE. Pour être sûr de répondre correctement aux questions du Générateur, vous devez connaître vos pratiques en matière de données de caractère personnel. Donc, avant de remplir le questionnaire, il est indispensable d'entreprendre **un examen interne approfondi** de vos pratiques actuelles en matière de **données à caractère personnel**. Par exemple :

- Recueillez-vous des données à caractère personnel ?
- Quels types de données à caractère personnel recueillez-vous ?
- Comment sont-elles recueillies ? Proviennent-elles d'individus, de tiers, d'entités publiques ou des autorités ? Les individus savent-ils que les données les concernant sont recueillies ?
- Qui, dans votre organisation, détermine quelles données à caractère personnel sont recueillies et comment elles sont recueillies ?
- Qui contrôle les données à caractère personnel, une fois qu'elles sont recueillies ?
- Les données à caractère personnel sont-elles divulguées à des tiers et, dans l'affirmative, pourquoi ?
- Comment et où sont-elles stockées ?
- Avez-vous des normes, lignes directrices ou règlements applicables à votre organisation, en ce qui concerne la collecte, le contrôle ou le transfert de données à caractère personnel ?
- Permettez-vous aux visiteurs d'avoir accès aux données à caractère personnel que vous possédez sur eux ?
- Qu'est-ce qui se passe si un visiteur a des questions concernant ses données personnelles ? Que faites-vous si un visiteur n'est pas satisfait de la manière dont vous répondez ?

Des conseils supplémentaires sur la conduite d'un examen interne sont disponibles sur les sites Web de SIIA, USCIB ou CSQ Model Code CAN/CSA-Q830.

Vous pourriez également consulter :

www.jipdec.or.jp/security/privacy/index-e.html
www.research.att.com/projects/p3p/propgen
www.the-dma.org
www.truste.org/wizard

2ÈME ÉTAPE. Lorsque vous aurez examiné vos pratiques actuelles en matière de données à caractère personnel :

- Vous devriez examiner les lois ou les dispositifs d'autorégulation qui sont susceptibles de s'appliquer à votre collecte et à votre utilisation de données à caractère personnel. Des **agences gouvernementales**, des **organisations non gouvernementales** ou des **entités privées** peuvent éventuellement fournir une aide à cet égard.

Il est recommandé d'examiner vos pratiques actuelles à la lumière de cette réglementation et de les modifier, si besoin est, pour en assurer la conformité.

UTILISATION DU GÉNÉRATEUR POUR ÉLABORER UNE DÉCLARATION DE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE

3ÈME ÉTAPE. Lorsque vous aurez déterminé quelles sont vos pratiques actuelles en matière de données à caractère personnel et examiné ces pratiques à la lumière de la réglementation, vous êtes en mesure de remplir les questions du Générateur. La section intitulée « Aide » fournit des explications sur les termes employés, des indications sur la conformité avec les **Lignes directrices de l'OCDE sur la protection de la vie privée** et, s'il y a lieu, des informations supplémentaires sur d'autres instruments nationaux, régionaux ou internationaux. Il est important de lire les **notes techniques** avant de répondre aux questions.

Lorsque vous aurez rempli le questionnaire avec autant de précision que possible, un projet de déclaration de politique de protection de la vie privée sera automatiquement créé. Il proposera des phrases préformatées fondées sur vos réponses/choix.

ÉVALUER LE PROJET DE DÉCLARATION DE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE

4ÈME ÉTAPE. Ensuite, vous devriez vérifier :

- Que le projet de déclaration de politique de protection de la vie privée traduit fidèlement les pratiques de votre organisation en matière de données à caractère personnel.
- Que la déclaration de politique de protection de la vie privée est conforme aux lois et aux dispositifs d'autorégulation applicables au plan national, régional et international.
- Que les erreurs ont été corrigées et que la déclaration se lit facilement.

AFFICHAGE DE LA DÉCLARATION DE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE SUR VOTRE SITE WEB

5ÈME ÉTAPE. Une fois que vous vous êtes assuré que votre déclaration de politique de protection de la vie privée est un reflet fidèle de vos pratiques en matière de données à caractère personnel et se conforme aux règlements applicables, vous devez envisager la manière de mettre cette déclaration à la disposition du public. Des règlements auxquels vous êtes assujetti peuvent éventuellement vous obliger à mettre votre déclaration à un emplacement spécifique, par exemple votre page d'accueil ou là où sont recueillies des données à caractère personnel. En l'absence de règlements spécifiques, vous pourriez par exemple choisir de créer un lien entre votre page d'accueil et votre déclaration de politique de protection de la vie privée ou entre les pages où vous recueillez des données à caractère personnel et votre déclaration. Les Lignes directrices de l'OCDE sur la protection de la vie privée recommandent que les individus puissent accéder à l'information concernant les pratiques en matière de données à caractère personnel sans effort excessif en termes de temps, de connaissances ou de coût. Vous pouvez désirer également créer des liens vers des sites Web pertinents afin que les visiteurs puissent être avertis des règlements applicables.

MISE EN GARDE : une fois que votre déclaration de politique est publiquement affichée, votre responsabilité légale peut être invoquée au cas où vous ne vous y conformeriez pas ou si cette déclaration n'était pas en conformité avec les règlements locaux en vigueur.

Suivre les étapes énumérées ci-dessus vous aidera à vous assurer que votre déclaration de politique reflète fidèlement vos pratiques en matière de protection de la vie privée et qu'elle est conforme aux règlements applicables.

□ Qu'est-ce que le Générateur de l'OCDE ?
Limites et conditions d'utilisation
□ Commencer le questionnaire

Aide à l'utilisation du Générateur de déclaration de politique de protection de la vie privée de l'OCDE

Notes techniques sur l'utilisation du générateur

Le générateur de déclaration de politique de protection de la vie privée de l'OCDE est un outil qui se présente sous la forme d'un questionnaire destiné à vous aider à formuler la politique de protection de la vie privée que vous appliquez sur les sites Web de votre organisation en générant une page Web (en format HTML), qui peut être téléchargée à la fin du questionnaire du générateur et indiquera les réponses que vous aurez fournies au questionnaire. Cette page Web, une fois que vous y aurez apporté les modifications voulues, pourra être exposée et liée au site Web de votre organisation.

Le questionnaire commence par une page de **connexion**, qui vous permet d'indiquer la tâche qui vous intéresse :

- **Créer** une nouvelle déclaration ; il vous sera attribué un **identificateur de déclaration** et l'on vous demandera un **mot de passe**.
- **Modifier** une déclaration existante ; vous devrez indiquer votre **identificateur de déclaration** et votre **mot de passe.**
- **Supprimer** une déclaration existante ; vous devrez indiquer votre **identificateur de déclaration** et votre **mot de passe.**

S'agissant de la création ou de la modification d'une déclaration, il vous sera posé une série de questions auxquelles vous devrez répondre en vous fondant sur les pratiques de votre organisation en matière de protection de la vie privée. Ces questions sont regroupées en 11 sections auxquelles vous pouvez avoir accès en utilisant les boutons **Précédent** et **Suivant** situés au bas de chaque page.

Le bouton **Suivant** sert également à enregistrer la page affichée. C'est pourquoi il est important de cliquer dessus pour vous assurer que le contenu de la page affichée ne sera pas perdu.

Vous trouverez au début de chaque section un bouton **Aide** qui vous fournit un lien vers des explications approfondies sur les questions de la section. Chaque fenêtre **Aide** se compose de deux parties : la première explique le principe applicable retenu par l'OCDE, tandis que la seconde fournit d'autres éléments d'information sur des termes précis contenus dans les questions, pour lesquels des hyperliens ont été créés. En lisant la fenêtre **Aide** avant de tenter de répondre aux questions de la section correspondante, vous serez sûr d'avoir compris la question correctement et serez en mesure d'y apporter la réponse reflétant fidèlement vos pratiques en matière de protection de la vie privée.

Le générateur conserve en permanence les réponses que vous donnez aux questions de chacune des pages du questionnaire, vous laissant la possibilité de les modifier ou de les supprimer ultérieurement ou à tout moment. Pour ce faire, vous n'avez qu'à conserver l'**identificateur de déclaration** ainsi que le **mot de passe** que vous aurez indiqués lors de la création de la déclaration. Veillez à n'utiliser que les boutons **Suivant** et **Précédent** à la fin de chaque page du générateur pour naviguer d'une page du questionnaire à l'autre, car ce sont ces boutons qui permettent au générateur de valider et d'enregistrer les réponses.

Note : A moins que vous ne les supprimiez, l'information et les réponses que vous fournissez seront conservées dans le serveur de l'OCDE pour vous permettre d'y revenir et de modifier votre projet de déclaration. Cependant, l'OCDE n'accèdera pas à cette information ni n'en fera usage, pour quelque motif que ce soit.

A la fin de la plupart des pages du questionnaire, vous trouverez un bouton **Prévisualisation**, qui vous permettra de visualiser le projet de déclaration de politique de protection de la vie privée produit

à partir des réponses que vous aurez fournies. La déclaration s'affichera dans une nouvelle fenêtre. Une fois que vous aurez pris connaissance de la fenêtre **Prévisualisation**, il faudra la fermer pour revenir au questionnaire.

Note : Le projet de déclaration généré par la fonction de prévisualisation ne comprendra pas les réponses provenant de la page en cours, à moins que le contenu de cette page n'ait été enregistré parce que vous aurez cliqué sur le bouton **Suivant**.

A la fin du questionnaire, vous pourrez télécharger le projet de déclaration que vous aurez produit à l'aide du générateur en cliquant sur le bouton **Télécharger la déclaration** :

- Choisissez l'option **Enregistrer sous** dans la fenêtre d'options de téléchargement de votre navigateur.
- Changez le nom de la page en lui attribuant un suffixe **.htm** ou **.html**.
- Choisissez l'endroit où vous voulez enregistrer le fichier de la déclaration.
- Cliquez sur le bouton **OK**.

Notes complémentaires

Si le générateur est inactif pendant une période de quatre heures, vous devrez de nouveau exécuter la procédure de connexion afin d'accéder aux réponses que vous aurez déjà fournies. De plus, toutes les réponses non validées seront perdues.

Le générateur utilise des témoins de session ("provisoires") pour maintenir le lien entre l'utilisateur et le serveur de l'OCDE pendant l'utilisation du générateur. Ces témoins **ne sont pas** conservés en permanence dans l'ordinateur de l'utilisateur **ni** utilisés pour enregistrer de l'information concernant ce dernier. Assurez-vous que votre navigateur Internet est configuré pour accepter des témoins (tout au moins des témoins provisoires).

A la création d'une nouvelle déclaration, le générateur vous demande de choisir un mot de passe pour éviter que d'autres utilisateurs ne puissent accéder à votre information. Veillez à ne pas laisser la fenêtre de mot de passe vierge, car cela permettrait à d'autres utilisateurs d'avoir accès à votre déclaration. Le serveur de l'OCDE n'utilise pas de connexion sécurisée pendant l'utilisation du générateur. Par conséquent, le trafic réseau entre l'utilisateur et le serveur de l'OCDE n'est pas crypté.

OCDE

Page de connexion Aide

Si vous souhaitez créer une nouvelle déclaration de politique, sélectionnez Créer une nouvelle déclaration. Si vous souhaitez reprendre la saisie d'une déclaration déjà commencée, choisissez Modifier une déclaration existante, puis entrer le code d'accès qui vous a été fourni lors de la création de votre déclaration.

Informations de connexion

○ Créer une nouvelle déclaration

○ Modifier une déclaration existante

Numéro de déclaration :

Mot de passe :

<< Précédent **Suivant >>**

○ Effacer une déclaration existante

Code d'accès de la déclaration :

Mot de passe :

Page de connexion Aide

Créer une nouvelle déclaration

Notez bien le numéro de déclaration qui figure ci-dessous : vous en aurez besoin pour la modifier ultérieurement. Entrez un mot de passe pour éviter qu'un tiers ne puisse accéder à la déclaration. Notez bien votre mot de passe.

Code d'accès de la déclaration :

Mot de passe :

Confirmer le mot de passe :

<< Précédent **Suivant >>**

Identification du site et de l'organisation responsable (section 1 sur 11, page 1) Aide

Ces informations figureront dans votre déclaration de protection de la vie privée afin d'informer les visiteurs de votre site Web sur votre organisation.

1.1 Informations sur votre organisation et sur le(s) site(s) Web pour le(s)quel(s) cette déclaration est créée

Raison sociale :	
Adresse :	
Ville :	
État/Province/Département (s'il y a lieu) :	
Code postal :	
Pays :	
Nom du maître du fichier :	
Activité(s) principale(s) de l'organisation :	
Adresse de votre (vos) site(s) Web :	

1.2. Souhaitez-vous que cette déclaration s'applique à une filiale de votre organisation ainsi qu'à son (ses) site(s) Web ?

○ OUI ○ NON

<< Précédent | Suivant >>

Informations sur votre organisation et votre site Web (section 1 sur 11, page 2) Aide

1.3 Informations sur la(les) filiale(s) de votre organisation et sur le(s) site(s) Web auxquels vous souhaitez que cette déclaration s'applique.

	Filiale 1	Filiale 2
Raison sociale de la filiale :		
Adresse :		
Ville :		
État/Province/Département (s'il y a lieu) :		
Code postal :		
Pays :		
Nom du maître du fichier :		
Activité(s) principale(s) de la filiale :		
Adresse des site(s) Web :		

<< Précédent | Suivant >> | Prévisualisation

Autorisation d'accès anonyme aux visiteurs (section 2 sur 11, page 1) Aide

2. Les visiteurs peuvent-ils accéder à votre page principale et consulter votre site Web sans fournir de données à caractère personnel (à l'exception des données nécessaires pour l'administration du système, comme les informations habituelles de connexion du protocole http) ?

○ OUI ○ NON

<< Précédent | Suivant >> | Prévisualisation

Caractéristiques d'interactivité de votre site Web (section 3 sur 11, page 1) Aide

3.1 Votre site permet-il à ses visiteurs de communiquer entre eux ou de publier des informations accessibles par d'autres ?

○ OUI ○ NON

3.2 Votre site Web fait-il appel à un fournisseur de services Web (par exemple une société qui collecte des données à caractère personnel pour diffuser des messages publicitaires) qui collecte des données nominatives sur vos visiteurs ?

○ OUI ○ NON

3.2.1 Si oui, veuillez indiquer le nom du fournisseur :

1	
2	
3	

<< Précédent | Suivant >> | Prévisualisation

Collecte automatique d'informations (section 4 sur 11, page 1) Aide

4.1 Votre site Web utilise-t-il des cookies ?

○ OUI ○ NON

4.2 Votre organisation ou votre site Web consignent-ils automatiquement les données à caractère personnel sur un journal par des moyens autres que des cookies (programmation par exemple) et est-il possible de faire le lien entre des données non nominatives consignées automatiquement avec des données nominatives sur un individu particulier ?

○ OUI ○ NON

Si oui, à quelle fin ?

	Administration technique du site Web
	Recherche et développement
	Gestion de la clientèle
	Marketing
	Cession de données à caractère personnel
	Autres (préciser)
1	
2	
3	

<< Précédent Suivant >> Prévisualisation

Collecte automatique d'informations (section 4 sur 11, page 2) Aide

4.3 Votre organisation ou son site Web établissent-ils un lien entre des informations non nominatives stockées dans des cookies et des données nominatives concernant une personne en particulier ?

○ OUI ○ NON

4.3.1 Si oui, à quelle fin ?

	Administration technique du site Web
	Recherche et développement
	Gestion de la clientèle
	Marketing
	Cession de données à caractère personnel
	Autres (préciser)
1	
2	
3	

<< Précédent | Suivant >> | Prévisualisation

Données collectées et finalité (section 5 sur 11, page 1) Aide

5.1 Votre organisation ou votre site Web collectent-ils des données à caractère personnel fournies volontairement par vos visiteurs lorsqu'ils utilisent vos services ?

○ OUI ○ NON

5.2 Votre organisation ou votre site Web collectent-ils des données à caractère personnel sur vos visiteurs provenant d'autres sources (fichiers ou organismes publics, organisations privées) ?

○ OUI ○ NON

<< Précédent | Suivant >> | Prévisualisation

Données collectées et finalité (section 5 sur 11, page 2) Aide

Vous avez indiqué dans les questions 4.2, 4.3, 5.1 ou 5.2 que vous collectez des données à caractère personnel sur vos visiteurs. Veuillez préciser comment et lesquelles.

5.3.1 Données nominatives primaires et renseignements professionnels

☐ Communiqués volontairement par chaque visiteur

☐ Provenant de fichiers ou d'organismes publics

☐ Obtenus auprès d'organisations privées

Données nominatives primaires	Administration technique du site Web	Recherche et développement	Gestion de la clientèle	Marketing	Cession de données à caractère personnel
Nom	☐	☐	☐	☐	☐
Sexe	☐	☐	☐	☐	☐
Adresse	☐	☐	☐	☐	☐
Adresse électronique	☐	☐	☐	☐	☐
Numéro de téléphone/télécopie	☐	☐	☐	☐	☐
Autres (préciser)	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Renseignements professionnels	Administration technique du site Web	Recherche et développement	Gestion de la clientèle	Marketing	Cession de données à caractère personnel
Employeur/organisation	☐	☐	☐	☐	☐
Titre	☐	☐	☐	☐	☐
Adresse	☐	☐	☐	☐	☐
Adresse électronique	☐	☐	☐	☐	☐
Numéro de téléphone/télécopie	☐	☐	☐	☐	☐
Autres (préciser)	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

5.3.2 Autres renseignements personnels et données de profil

☐ Communiqués volontairement par chaque visiteur
☐ Provenant de fichiers ou d'organismes publics
☐ Obtenus auprès d'organisations privées

	Administration technique du site Web	Recherche et développement	Gestion de la clientèle	Marketing	Cession de données à caractère personnel
Données personnelles	☐	☐	☐	☐	☐
Description physique	☐	☐	☐	☐	☐
Situation familiale	☐	☐	☐	☐	☐
Niveau d'études et compétences	☐	☐	☐	☐	☐
Style de vie, goûts	☐	☐	☐	☐	☐
Ressources financières	☐	☐	☐	☐	☐
Autres (préciser)	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

5.3.3. Identificateurs

☐ Communiqués volontairement par chaque visiteur
☐ Provenant de fichiers ou d'organismes publics
☐ Obtenus auprès d'organisations privées

	Administration technique du site Web	Recherche et développement	Gestion de la clientèle	Marketing	Cession de données à caractère personnel
Données d'identification en ligne	☐	☐	☐	☐	☐
Données d'identification financière	☐	☐	☐	☐	☐
Identificateurs affectés par des organismes publics	☐	☐	☐	☐	☐
Identificateurs biométriques	☐	☐	☐	☐	☐
Autres (préciser)	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

5.3.4 Données spécifiques

- ☐ Communiqués volontairement par chaque visiteur
- ☐ Provenant de fichiers ou d'organismes publics
- ☐ Obtenus auprès d'organisations privées

	Administration technique du site Web	Recherche et développement	Gestion de la clientèle	Marketing	Cession de données à caractère personnel
Origine raciale ou ethnique	☐	☐	☐	☐	☐
Opinions politiques	☐	☐	☐	☐	☐
Croyances religieuses ou philosophiques	☐	☐	☐	☐	☐
Appartenance syndicale	☐	☐	☐	☐	☐
Informations médicales	☐	☐	☐	☐	☐
Pratiques sexuelles	☐	☐	☐	☐	☐
Données policières ou judiciaires (assignations en justice par exemple)	☐	☐	☐	☐	☐
Autres (préciser)	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

<< Précédent **Suivant >>** **Prévisualisation**

Données collectées et finalité (section 5 sur 11, page 3) Aide

5.4 Collectez-vous des données dans une autre finalité ?

○ OUI ○ NON

5.4.1 Si oui, avec quelle(s) autre(s) finalité(s) collectez-vous des données ?

1	
2	
3	

5.5. Si vous souhaitez utiliser les données personnelles de vos visiteurs dans des finalités autres que celles que vous avez indiquées précédemment dans ce questionnaire, donnez-vous à vos visiteurs la possibilité de donner leur consentement à ces autres utilisations ?

○ OUI ○ NON

5.5.1 Si oui, comment vos visiteurs peuvent-ils exprimer leur choix ?

	En cochant une case à l'endroit de votre site où les données sont collectées	
	En envoyant un message électronique. Indiquez l'adresse e-mail	
	En visitant une page Web. Indiquez son adresse Web	
	En envoyant un courrier postal. Indiquer à quelle adresse	
	En composant un numéro de téléphone. Indiquez le numéro de téléphone	
	Par d'autres voies (préciser)	

<< Précédent | Suivant >> | Prévisualisation

Protection des données concernant les mineurs (section 6 sur 11, page 1) Aide

6.1 Collectez-vous délibérément des données personnelles sur des mineurs ?

○ OUI ○ NON

6.2 Prenez vous des mesures spécifiques pour protéger la vie privée des mineurs sur lesquels vous collectez des données (délibérément ou non délibérément) ?

○ OUI ○ NON

5.4.1 Si oui, veuillez préciser des mesures spécifiques vous prenez pour protéger la vie privée des mineurs, en choissent tous les cases relevants :

	Nous faisons en sorte, dans la mesure du possible, de vérifier qu'un parent a donné son consentement à la collecte de données personnelles sur le mineur.
	Nous offrons la possibilité au parent de donner son consentement à la collecte et à l'utilisation des données personnelles concernant l'enfant en vue d'une utilisation en interne.
	Nous offrons la possibilité au parent de donner son consentement à la collecte et à l'utilisation des données personnelles concernant l'enfant en vue de les communiquer à des tiers.

Autres mesures (préciser, par exemple : Afin de protéger la vie privée des mineurs sur notre site Web, nous…)

1	
2	
3	

6.6.2 Présentez-vous, sur votre page principale et toutes les pages où vous collectez des données personnelles sur les mineurs, des informations sur vos pratiques en matière de données personnelles relatives aux mineurs ?

○ OUI ○ NON

<< Précédent | Suivant >> | Prévisualisation

Divulgation des données et choix du visiteur (section 7, page 1) Aide

7.1 Votre organisation divulgue-t-elle à ses filiales ou à d'autres organisations des données personnelles sur les visiteurs du site Web ?

○ OUI ○ NON

<< Précédent | Suivant >> | Prévisualisation

Divulgation des données et choix du visiteur (section 7, page 2) Aide

7.2 Lorsque vous divulguez des données personnelles pour les finalités que vous avez indiquées précédemment dans ce questionnaire, donnez-vous aux visiteurs la possibilité de :

☐ Donner leur consentement explicite à la divulgation de données personnelles

Et/ou

☐ Signifier leur refus

7.2.1 Si vous offrez aux visiteurs le choix de consentir ou de refuser de vous communiquer des données personnelles, comment ce choix est-il exprimé ?

	En cochant une case à l'endroit où sont collectées les données personnelles	
	En envoyant un message électronique. Indiquez l'adresse e-mail	
	En visitant une page Web. Indiquez son adresse Web	
	En envoyant un courrier postal. Indiquer à quelle adresse	
	En composant un numéro de téléphone. Indiquez le numéro de téléphone	
	Par d'autres voies (préciser)	

7.3 Lorsque vous divulguez des données personnelles dans des finalités autres que celles que vous avez indiquées précédemment dans ce questionnaire, offrez-vous aux visiteurs la possibilité de consentir à cette divulgation ?

○ OUI ○ NON

7.3.1 Si oui, comment ce consentement est-il exprimé ?

	En cochant une case à l'endroit où sont collectées les données personnelles	
	En envoyant un message électronique. Indiquez l'adresse e-mail	
	En visitant une page Web. Indiquez son adresse Web	
	En envoyant un courrier postal. Indiquer à quelle adresse	
	En composant un numéro de téléphone. Indiquez le numéro de téléphone	
	Par d'autres voies (préciser)	

<< Précédent | Suivant >> | Prévisualisation

Confidentialité et sécurité (section 8 sur 11, page 1) Aide

8.1 Donnez-vous la possibilité aux visiteurs de votre site d'utiliser une méthode de transmission sécurisée pour vous envoyer des données personnelles ?

○ OUI ○ NON

8.2 Veuillez cocher les cases correspondant aux catégories de données personnelles que vos visiteurs peuvent vous envoyer par une méthode de transmission sécurisée :

	Données personnelles primaires (nom et coordonnées)
	Autres données personnelles de profil (description physique, loisirs)
	Identificateurs (numéro de carte de crédit, mot de passe du site Web)
	Données personnelles spécifiques (origine raciale ou ethnique, croyances religieuses, données médicales)

Autres (préciser) :

1	
2	
3	

8.3 Votre site Web obéit-il à une politique, des règles ou des mesures de sécurité visant à protéger les renseignements que vous détenez sur les visiteurs contre les risques suivants :

8.3.1	Accès non autorisés	○ OUI	○ NON
8.3.2	Utilisation ou divulgation abusives	○ OUI	○ NON
8.3.3	Modifications ou altérations non autorisées	○ OUI	○ NON
8.3.4	Destruction illicite ou perte accidentelle	○ OUI	○ NON

8.4 Vos salariés et les personnes qui traitent les données sont-ils tenus de respecter la confidentialité des données personnelles concernant les visiteurs ?

○ OUI ○ NON

8.5 Votre organisation et votre site garantissent-ils que les données personnelles concernant les visiteurs collectées sur son site Web ne seront pas divulguées à des institutions ou à des autorités gouvernementales, hormis dans les cas prévus par la loi ou la réglementation ?

○ OUI ○ NON

<< Précédent | Suivant >> | Prévisualisation

Participation individuelle/ accès (section 9 sur 11, page 1) Aide

9.1 Un visiteur peut-il savoir, en s'adressant à votre organisation ou par l'intermédiaire de votre site Web, si vous détenez des données personnelles le concernant ?

○ OUI ○ NON

9.1.1 Si oui, par quels moyens peut-il le faire ?

	En envoyant un message électronique. Indiquez l'adresse e-mail	
	En visitant une page Web. Indiquez son adresse Web	
	En envoyant un courrier postal. Indiquer à quelle adresse	
	En composant un numéro de téléphone. Indiquez le numéro de téléphone	
	Par d'autres voies (préciser)	

9.2 Un visiteur peut-il obtenir de votre organisation (sur votre site Web) une copie intelligible des données personnelles que vous détenez sur lui ?

○ OUI ○ NON

9.2.1 Si oui, par quels moyens peut-il faire cette demande ?

	En envoyant un message électronique. Indiquez l'adresse e-mail	
	En visitant une page Web. Indiquez son adresse Web	
	En envoyant un courrier postal. Indiquer à quelle adresse	
	En composant un numéro de téléphone. Indiquez le numéro de téléphone	
	Par d'autres voies (préciser)	

9.2.2 Dans quels délais les visiteurs obtiennent-ils généralement ces informations ?

- ☐ Presque instantanément en ligne
- ☐ En une semaine
- ☐ En un mois
- ☐ Dans un délai plus long (préciser)

9.2.3 Ce service est-il payant ?

○ OUI ○ NON

9.2.4 Dans l'affirmative, combien est-il facturé :

9.3 Un visiteur peut-il contester les données que vous détenez sur lui ?

○ OUI ○ NON

9.3.1 Dans l'affirmative, le visiteur peut-il demander que ses données personnelles soient (selon les cas) :

- ☐ Effacées
- ☐ Rectifiées ou modifiées
- ☐ Complétées

9.4 Vous réservez-vous le droit de refuser à un visiteur de lui communiquer les données le concernant ?

○ OUI ○ NON

9.4.1 Si oui, motivez-vous votre refus au visiteur ?

○ OUI ○ NON

9.4.2 En cas de refus de lui communiquer les données personnelles que vous détenez, le visiteur a-t-il la possibilité de contester ce refus?

○ OUI ○ NON

9.5 Demandez-vous que le visiteur apporte la preuve de son identité avant de lui communiquer ses données personnelles ?

○ OUI ○ NON

<< Précédent **Suivant >>** **Prévisualisation**

Normes de confidentialité (section 10 sur 11, page 1) Aide

10.1 Existe-t-il une législation nationale ou des normes professionnelles applicables à votre site Web ou à votre organisation en matière de confidentialité ?

○ OUI ○ NON

10.1.1 Si oui, votre politique en matière de confidentialité est-elle conforme à la législation nationale ou aux normes professionnelles ?

○ OUI ○ NON

10.1.2 Veuillez indiquez le(s) principa(ux)l instrument(s) de protection de la vie privée au(x)quel(s) se conforme votre politique (titre et pays dans chaque champ) :

1	
2	
3	

10.2 Existe-t-il des normes mondiales, régionales ou professionnelles en matière de confidentialité qui s'appliquent à votre site web ou à votre organisation ?

○ OUI ○ NON

10.2.1 Si oui, votre politique en matière de confidentialité est-elle conforme à la législation mondiale ou régionale ou aux normes professionnelles ?

○ OUI ○ NON

10.2.2 Veuillez indiquer les principales normes mondiales, régionales ou professionnelles en matière de confidentialité qui s'appliquent à votre site Web ou à votre organisation (titre et origine dans chaque champ) :

1	
2	
3	

10.3 Pour démontrer que votre politique en matière de respect de la vie privée est bien conforme à la réglementation applicable mentionnée ci-dessus :

	Vous soumettez volontairement vos pratiques à une procédure d'auto-évaluation
	Vous êtes soumis volontairement à une certification par un organisme tiers
	Vous êtes soumis à la surveillance d'une agence de tutelle gouvernementale
	Vous êtes soumis à la surveillance d'une autorité indépendante chargée de la protection des données

10.3.1 Veuillez préciser les éléments suivants selon votre situation :

Procédure d'auto-évaluation

Nom ou fonction de la personne ou du service responsable de la politique de la protection de la vie privée	
Adresse Web	
Adresse	
Pays	

Certification par un organisme tiers

Désignation de l'organisation	
Adresse Web	
Adresse	
Pays	

Agence de tutelle gouvernementale

Désignation de l'agence	
Adresse Web	
Adresse	
Pays	

Autorité indépendante chargée de la protection des données

Désignation de l'autorité	
Adresse Web	
Adresse	
Pays	

<< Précédent **Suivant >>** **Prévisualisation**

Points de contact sur la protection de la vie privée (section 11 sur 11, page 1) Aide

11.1 Votre site Web indique-t-il aux visiteurs la personne à contacter pour les questions ou problèmes en matière de protection de la vie privée ?

○ OUI ○ NON

11.1.1 Veuillez indiquer les informations suivantes sur la personne à contacter :

	Contact 1	Contact 2
Nom ou fonction :		
Service :		
Adresse :		
Numéro de téléphone :		
Numéro de télécopie :		
Adresse électronique :		
Adresse Web :		

11.2 Si un visiteur n'est pas satisfait de votre réponse, lui indiquez-vous par quels autres moyens il pourrait obtenir satisfaction ?

○ OUI ○ NON

11.3 Quels autres moyens d'obtenir satisfaction indiquez-vous ?

☐ Si votre organisation ou votre site Web propose aux utilisateurs de recourir à un mécanisme de résolution des différents faisant appel à un tiers pour les affaires liées à la collecte ou à l'utilisation d'informations nominatives les concernant, veuillez indiquer les noms et coordonnées de ces services ainsi que leurs conditions d'accès.

Nom :	
Cordonnées (ex : adresse Web) :	
Conditions d'accès (ex : frais) :	

☐ Contact avec une agence ou une administration publique. Veuillez indiquer ses nom et coordonnées.

Nom :	
Cordonnées (ex : adresse Web) :	

☐ Contact avec une autorité de protection des données. Veuillez indiquer ses nom et coordonnées.

Nom :	
Cordonnées (ex : adresse Web) :	

☐ Autre. Veuillez préciser (Si un visiteur n'est pas satisfait de notre réponse à leurs craintes, nous lui recommander de contacter….):

Nom :	
Cordonnées (ex : adresse Web) :	

<< Précédent **Suivant >>** **Prévisualisation**

Accéder à votre projet de déclaration Aide

Maintenant que vous avez rempli le questionnaire un projet de déclaration va être généré en fonction de vos réponses. Veuillez lire ce qui suit et prévisualiser votre projet de déclaration au bas de cette page avant de le télécharger.

1. Évaluer le contenu de votre projet de déclaration

Assurez vous :

- Que votre projet de déclaration traduit fidèlement les pratiques de votre organisation en matière de données à caractère personnel.
- Qu'il est conforme aux lois et aux dispositifs d'autorégulation applicables aux plans national, régional et international.
- Que votre déclaration se lit facilement et ne comporte aucune erreur.

2. Vérifier que votre projet de déclaration de politique de protection de la vie privée est bien conforme aux Principes directeurs de l'OCDE

Votre projet de déclaration sera généré en fonction des réponses que vous avez apportées aux questions.

Si les réponses que vous avez apportées ne sont pas conformes aux Principes directeurs de l'OCDE en matière de protection de la vie privée, des commentaires seront générés à la fin de votre projet de déclaration. Ils apparaîtront en **rouge** de façon à être immédiatement repérables.

Si un tel commentaire apparaît à la fin de votre projet de déclaration, peut-être souhaiterez-vous retourner à la question correspondante du questionnaire et envisager de modifier vos pratiques en matière de protection de la vie privée. Le cas échéant, une fois ces adaptations effectuées et mises en œuvre, vous pourrez changer vos réponses afin d'actualiser votre déclaration.

3. Modifier votre projet de déclaration

- NOUS VOUS RAPPELONS que vous êtes tenu de faire preuve d'équité et de bonne foi en ce qui concerne le Générateur et le contenu des déclarations qu'il produit.
- NOUS VOUS RAPPELONS que l'utilisation du Générateur ne saurait en aucune manière impliquer que l'OCDE approuve ou avalise votre politique de protection de la vie privée et la déclaration que vous avez élaborée.
- Si vous souhaitez que votre déclaration fasse référence à l'OCDE ou au Générateur, VEUILLEZ INDIQUER CLAIREMENT que vous avez utiliser le générateur de l'OCDE dans le cadre de l'élaboration de votre politique de protection de la vie privée et de votre déclaration, et placer un lien vers le générateur.

4. Mettre votre déclaration de politique de protection de la vie privée en ligne

- UNE FOIS que vous êtes satisfait du projet de déclaration vous pouvez effacer toute référence à sa qualité de "projet" et les éventuels commentaires en rouge avant de mettre votre déclaration en ligne sur votre site Web.
- N'OUBLIEZ PAS que la législation qui vous est applicable en matière de protection de la vie privée exige peut-être que votre déclaration de politique figure en certains points de votre site Web.
- En l'absence de dispositions réglementaires particulières, vous pouvez créer des hyperliens vers votre déclaration de protection de la vie privée depuis votre page d'accueil ou depuis les pages où sont collectées les données personnelles. Vous pouvez aussi créer des liens vers différents sites Web permettant aux visiteurs de s'informer de certaines dispositions pertinentes.

Télécharger la déclaration

<< Précédent **Suivant >>** **Prévisualisation**

Chapitre 8

RENFORCER LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE : LE RÈGLEMENT DES LITIGES ENTRE ENTREPRISES ET CONSOMMATEURS COMPTE RENDU DE LA CONFÉRENCE DE L'OCDE TENUE EN DÉCEMBRE 2000

Ce chapitre résume une conférence sur le règlement des litiges en ligne entre entreprises et consommateurs, conjointement avec la Conférence de La Haye de droit international privé (CODIP) et la Chambre de commerce internationale (CCI), qui a eu lieu les 11 et 12 décembre 2000 à La Haye. La Conférence avait un triple objectif : *(i)* permettre la présentation, l'analyse et la diffusion d'informations sur le large éventail de mécanismes existants pour le règlement alternatif des litiges (RAL) en ligne ; *(ii)* voir si et comment le règlement des litiges en ligne peut aider à régler les différends de commerce électronique grand public liés au respect de la vie privée et à la protection des consommateurs, et améliorer ainsi la confiance dans le commerce électronique mondial ; et *(iii)* analyser le rôle des divers acteurs dans le développement de mécanismes appropriés et efficaces de règlement alternatif des litiges en ligne. Le thème principal de la conférence était les litiges de commerce électronique entre entreprises et consommateurs impliquant des transactions de faible valeur ou des préjudices de faible importance, et les systèmes informels et flexibles permettant de concilier au mieux la nature du litige et le formalisme de la procédure de règlement (par exemple, négociation assistée et médiation). Le rapport de la conférence est précédé par le document d'orientation sur lequel les participants à la conférence se sont appuyés pour examiner les différents thèmes.

Chapitre 8

RENFORCER LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE : LE RÈGLEMENT DES LITIGES ENTRE ENTREPRISES ET CONSOMMATEURS COMPTE RENDU DE LA CONFÉRENCE DE L'OCDE TENUE EN DÉCEMBRE 2000

Présentation de la conférence (document d'orientation et présentation du programme)

L'environnement en ligne joue un rôle important sur le marché mondial. Les consommateurs comme les entreprises tireront d'importants avantages des échanges en ligne. Mais parallèlement à ces avantages et à l'augmentation attendue des échanges nationaux et internationaux de commerce électronique entre entreprises et consommateurs apparaissent de nouveaux défis, liés notamment à la détermination du droit applicable et de la juridiction compétente ou au droit à réparation au-delà des frontières. Étant donné que les mécanismes traditionnels judiciaires de règlement des litiges pourraient ne pas être un moyen efficace de réparation pour les échanges de commerce électronique, il convient d'étudier les mécanismes alternatifs déjà en usage ou en cours de développement.

Les modes alternatifs de règlement des litiges en ligne offrent en effet la perspective d'un règlement rapide et peu onéreux pour nombre de petites réclamations et de transactions de faible valeur générées par le commerce entreprises-consommateurs en ligne. De plus, on peut compter sur les progrès de la technologie pour fournir en permanence des solutions novatrices et potentiellement plus efficaces de règlement des litiges, indépendamment des mécanismes existants ou en liaison avec ces derniers.

Cette Conférence sur le règlement en ligne des litiges entre entreprises et consommateurs est organisée conjointement par l'OCDE[1], la Conférence de La Haye de droit international privé (CODIP) et la Chambre de Commerce Internationale (CCI). Le point de vue des consommateurs sera représenté par Consumer International (CI).

Objectifs

S'appuyant sur les débats et les éléments réunis à ce jour dans divers forums, la conférence va :

- Permettre de présenter, analyser et diffuser des informations sur la diversité des modes alternatifs de règlement des litiges en ligne (1er jour).
- Étudier si et comment les modes alternatifs de règlement des litiges en ligne peuvent améliorer la confiance à l'égard du commerce électronique mondial en aidant à résoudre les litiges entre entreprises et consommateurs qui concernent les questions de respect de la vie privée et de protection des consommateurs ; il s'agit de déterminer les éléments que les acteurs considèrent comme importants pour l'équité et l'efficacité des modes alternatifs de règlement des litiges en ligne, étant entendu que ces éléments, qui sont de nature diverse (socio-économiques, juridiques et techniques), peuvent varier suivant le type de mécanisme et/ou litige.
- Examiner le rôle des acteurs pour faciliter l'adoption de modes appropriés et efficaces de règlement des litiges en ligne (2e jour).

Analyse et travaux futurs des co-organisateurs

Pendant les deux jours de débats, la conférence devrait aider les acteurs à définir leurs nouveaux axes de travail. Le Secrétariat établira des propositions de travaux futurs pour l'OCDE dans le domaine des modes alternatifs de règlement des litiges en ligne, lesquelles seront présentées au Groupe de travail sur la sécurité de l'information et la vie privée et au Comité de la politique à l'égard des consommateurs à leurs prochaines réunions début 2001.

Déroulement de la conférence

La conférence a été organisée de manière à faciliter les débats entre les participants aux différentes sessions et avec le public. Sous la conduite de modérateurs, la plupart des sessions commenceront par de brèves présentations, suivies des réactions et commentaires des membres des commissions, et se poursuivront par des questions-réponses avec la participation active de l'assistance. Un large éventail d'acteurs, notamment des représentants des entreprises, des usagers, des consommateurs et des gouvernements participeront à la conférence. Y participeront aussi des universitaires et des prestataires de règlement alternatif.

Documents de référence

Le présent document d'orientation est destiné à aider les participants à la conférence à débattre des questions à étudier. Il souligne les principaux points à aborder lors de chaque session de la conférence, propose les questions à examiner et contient un bref résumé des présentations. On trouvera, joints en annexe, les documents suivants :

- Liste des modes de règlement alternatif des litiges en ligne recensés par l'OCDE (en fonction de travaux de recherche indépendants et d'éléments fournis par la CCI et CI), valable pour octobre 2000 (appendice A).

- Liste des éventuels éléments procéduraux, substantiels et autres que pourraient comporter les modes alternatifs de règlement des litiges en ligne (appendice B).

- Différents articles et recommandations ont trait aux modes alternatifs de règlement des litiges en ligne, entre entreprises et consommateurs, élaborés jusqu'à présent par les organismes suivants :

    - Commission européenne (CE) (Recommandation 98/257/CE de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation).
    - Dialogue Transatlantique avec les Consommateurs (DTAC) (règlement alternatif des litiges dans le contexte de la recommandation sur le commerce électronique de février 2000).
    - Commission européenne (CE) (les systèmes de règlement extrajudiciaire des litiges pour le commerce électronique : rapport de l'atelier organisé à Bruxelles le 21 mars 2000).
    - Gouvernement des États-Unis (résumé de l'atelier public de juin 2000 « règlement alternatif des litiges concernant les transactions de consommation sur un marché électronique sans frontières » novembre 2000).

- Groupe de direction de la Coopération économique Asie Pacifique (APEC) sur le commerce électronique : rapport et propositions d'action à l'issue de l'atelier de l'APEC sur la protection des consommateurs organisé à Bangkok le 20 juillet 2000).
- Dialogue mondial des entreprises sur le commerce électronique (règlement alternatif des litiges, document de septembre 2000).
- Consumers International (CI) (Rapport sur les litiges dans le cyberespace, décembre 2000).

- Rapports et documents ayant trait au règlement alternatif des litiges et aux programmes de label de confiance :

  - Rapport de la table ronde de Genève, de septembre 1999, sur le commerce électronique et le droit international privé, avril 2000.
  - Lignes directrices du Groupe sur le commerce électronique et la protection des consommateurs pour les transactions entre négociants et consommateurs, diffusées le 6 juin 2000.
  - Inventaire des mécanismes de règlement alternatif des litiges en ligne établi par la CCI dans «règlement extrajudiciaire des litiges portant sur les transactions de commerce électronique des consommateurs : inventaire des approches actuelles, septembre 2000».
  - Rapport sur la «sécurité du Web : étude des programmes concernant la protection de la vie privée» en ligne, établi par les Commissaires à la protection des données de l'Ontario, Canada et Australie, septembre 2000.
  - Code BBB en ligne des pratiques en ligne des entreprises, diffusé le 24 octobre 2000.

- Articles et commentaires transmis spontanément par le public en prévision des débats de la conférence.

Présentation du règlement alternatif des litiges

L'expression règlement alternatif des litiges renvoie à un large éventail de mécanismes et de procédures destinés à aider les parties à résoudre leurs différends. Ces mécanismes alternatifs ne sont pas destinés à remplacer les tribunaux, mais à les compléter.[2] Généralement, un mode alternatif de règlement des litiges comporte une série de procédures dont certaines peuvent varier selon la forme du règlement[3]. Les formes les plus courantes de règlement sont la négociation, la facilitation ou la conciliation, la médiation et l'arbitrage.

Bien qu'il n'y ait pas total consensus dans les milieux universitaires ou dans le monde des affaires sur la définition précise des modes alternatifs de règlement des litiges, la plupart des spécialistes considèrent le règlement alternatif comme un éventail de moyens d'action qui s'inscrivent dans le cadre plus large du règlement des litiges, à savoir les différents moyens de régler les litiges : services consommateurs des sociétés, règlement alternatif des litiges et action en justice. Les modes alternatifs de règlement des litiges varient sur une échelle mobile des plus souples aux plus officiels sur le plan des règles de procédure et en fonction des éléments suivants : le rôle de tiers neutres pour faciliter un règlement ou trancher le litige, le caractère contraignant ou non du règlement pour toutes les parties ou l'une d'entre elles et, en cas de caractère contraignant, le fait qu'il en ait été ou non convenu préalablement, avant ou après la survenance du litige.

Aux deux extrêmes du règlement alternatif des litiges on trouve la négociation assistée[4] (la plus informelle) et l'arbitrage[5] (le plus formel, ou le plus « quasi judiciaire »). Par exemple, dans la négociation assistée, les décisions restent à tous moments dans les mains des parties et les solutions

sont définies d'un commun accord. En revanche, dans l'arbitrage, les parties décident d'être tenues par la décision définitive de l'arbitre avant ou après la survenance du litige. Entre négociation assistée et arbitrage, il existe une grande variété de formes de médiation, de l'évaluation neutre aux formes hybrides comme la médiation-arbitrage (médarb).

Le règlement alternatif des litiges sert à résoudre hors-ligne de nombreuses formes de litiges, des différends de voisinage aux transactions commerciales internationales. Il n'est pas étonnant que des mécanismes de règlement alternatif se développent dans l'environnement en ligne pour régler un large éventail de litiges (noms de domaine, assurance, vie privée, famille, emploi et aspects commerciaux) entre parties (entreprises-entreprises, entreprises-consommateurs, consommateurs-consommateurs, administrations-entreprises et administrations-consommateurs) qui surviennent dans les échanges électroniques. Ces mécanismes en ligne ne concernent pas seulement les litiges qui surviennent en ligne : en effet, un différend qui se produit hors ligne peut être résolu par un mécanisme de règlement en ligne.

Le règlement alternatif des litiges en ligne intervient dans de nombreux contextes, notamment sur un marché électronique particulier (ex. : site de vente aux enchères en ligne), sous forme d'une marque de confiance ou d'un programme de garantie, ou à titre indépendant. Ces différences peuvent avoir un effet sur l'accès des consommateurs au règlement alternatif des litiges et le respect de la solution par les entreprises.

Dans les enquêtes et les inventaires récents, l'OCDE, la CCI et CI ont recensé plus de 40 mécanismes alternatifs de règlement des litiges en ligne, la plupart offrant un règlement entre entreprises et consommateurs[6]. Ces mécanismes alternatifs de règlement des litiges en ligne varient en fonction de leurs aspects procéduraux et techniques. Toutefois, il est possible de distinguer ceux qui sont complètement automatisés dans la mesure où les solutions sont élaborées par un logiciel informatique et sans intervention humaine et la plupart des autres, qui se répartissent en fonction de leur degré de formalisme. Si 26 des prestataires de règlement alternatif de litiges en ligne offrent un règlement informel et dénué de caractère contraignant comme la négociation assistée, la médiation ou les services de type médiateur, 14 mettent à disposition des procédures d'arbitrage plus formelles à caractère contraignant : 11 proposent le règlement automatisé des litiges et 14 offrent de multiples modes alternatifs de règlement des litiges en ligne.

Thème central

La présente conférence étudiera l'utilisation des modes alternatifs de règlement des litiges en ligne pour les différends portant sur un faible montant et entraînant un faible préjudice, qui se produisent en ligne entre entreprises et consommateurs. On s'attachera surtout aux systèmes informels et souples qui ménagent l'équilibre nécessaire entre le type de litige et le formalisme de la procédure de règlement (voir la zone grisée dans la figure ci-dessous). Par exemple, le coût ou la complexité de la procédure ne doivent pas être disproportionnés par rapport à ce qui est en jeu.

Figure 8.1. **Principaux types et principales procédures de règlement alternatif des litiges**

Services de réclamation interne	Négociation assistée	Médiation	Arbitrage	Action en justice
	– Facilitation – Conciliation	***Sur une échelle mobile :*** – Automatisée, ou non – Intervention plus ou moins active du tiers neutre – Participation volontaire ou obligatoire – Pas d'obligation pour les parties d'accepter avant de participer au règlement alternatif que la solution les engagera	– Soumission volontaire ou obligatoire – Automatisé ou non – Définitif et obligatoire	
	→→→→→→→→→ **règlement alternatif des litiges, d'informel à formel**			

Source: OECD.

Premier jour : panorama des modes alternatifs de règlement des litiges en relation avec l'environnement en ligne

Accueil et allocution de bienvenue

Renforcer la confiance est un enjeu important pour la nouvelle économie et la société mondiale de l'information. En particulier, l'élément clé du renforcement de la confiance consiste à garantir aux usagers et aux consommateurs la possibilité d'obtenir réparation pour les litiges résultant d'échanges et de transactions de commerce électronique.

Le mandat de l'OCDE concernant l'étude des modalités de réparation des préjudices subis par les usagers et les consommateurs est clairement énoncé dans la Déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux[7] et dans la Recommandation relative à la protection des consommateurs dans le contexte du commerce électronique[8], qui fixent les grandes lignes des travaux de l'OCDE sur le commerce électronique. Ce mandat est précisé dans les Lignes directrices de 1999 sur la protection des consommateurs dans le contexte du commerce électronique, par lesquelles les pays membres de l'OCDE soulignent l'importance d'assurer aux consommateurs « un accès effectif à des voies de règlement des litiges et de recours justes et rapides sans charge ni coûts indus »[9]. De même, le besoin de mécanismes adéquats de règlement des litiges concernant la vie privée a été mis en exergue dans le rapport de l'OCDE sur les contrats de flux de données transfrontières dans le cadre plus large des mécanismes de protection de la vie privée sur les réseaux mondiaux[10].

Par conséquent, le programme de travail de l'OCDE pour 2000-2001 met l'accent sur l'examen des modalités de règlement efficace des litiges relatifs à la protection des consommateurs et de la vie privée par le biais des modes alternatifs de règlement des litiges en ligne.

Allocution de bienvenue

A.H Korthals, Ministre de la Justice, Pays-Bas

Discours introductifs

Pourquoi le règlement alternatif des litiges est-il un élément clé du renforcement de la confiance dans l'environnement en ligne ?

Herwig Schlögl, Secrétaire général adjoint, Organisation de Coopération et de Développement Économiques

L'importance d'un partenariat mondial dans le développement et le soutien des modes alternatifs de règlement des litiges

Marcia Livanos Cattaui, Secrétaire général, Chambre de Commerce Internationale

Au tribunal ou hors tribunal ? Défis pour la Conférence de La Haye

Hans van Loon, Secrétaire général, Conférence de La Haye de droit international privé

Remarques liminaires par le Président de la première journée

Peter Ford, Président, Groupe de travail sur la sécurité de l'information et la vie privée

Session 1 : État des lieux – panorama des récentes discussions à propos du règlement alternatif des litiges en ligne

Plusieurs entités ont défini des principes concernant les systèmes alternatifs de règlement des litiges en ligne entre entreprises et consommateurs ou exprimé des points de vue sur les éléments essentiels de ces systèmes. Afin d'offrir un forum, au niveau mondial, pour l'étude des modes alternatifs de règlement des litiges en ligne et d'encourager la coopération entre les acteurs, cette session fera le point des travaux qui ont été entrepris sur ce thème par d'autres organisations. Des représentants de la Commission européenne (CE), des États-Unis, de la Coopération économique Asie-Pacifique (APEC), du Dialogue mondial des entreprises et de Consumers International (CI) seront invités à présenter les résultats des travaux de leurs organisations sur les modes alternatifs en ligne.

Bien qu'il y ait un terrain d'entente sur les principes de règlement alternatif des litiges en ligne, les débats doivent se poursuivre. Cette session tentera de mettre en lumière les similitudes et les différences qui existent entre les différentes approches connues à ce jour afin de faciliter l'examen des défis à relever et des lacunes à combler pour un règlement alternatif juste et efficace des litiges en ligne.

Modérateur : Risaburo Nezu, Directeur, Direction de la Science, la Technologie et l'Industrie, OCDE

Présentateurs :

Carina Tornblom, Chef de service, Direction générale de la protection de la santé et des consommateurs. La Commission européenne présentera son approche fondée sur la recommandation de 1998 concernant les principes applicables aux organismes responsables du règlement hors tribunal pour la résolution extrajudiciaire des litiges de consommation et les travaux de l'atelier organisé en mars 2000[11].

James Dorskind, Jurisconsulte, Ministère du commerce des États-Unis, donnera un aperçu du rapport récemment diffusé à l'issue de l'atelier public commun de la Commission fédérale du commerce et du Ministère du commerce, intitulé « Règlement alternatif des litiges relatifs aux transactions des

consommateurs dans un marché en ligne sans frontières », organisé à Washington, DC les 6 et 7 juin 2000[12].

Yuko Yasunaga, Directeur adjoint, Division de la politique du commerce, Ministère japonais du commerce international et de l'industrie (APEC), présentera les résultats de l'atelier APEC sur la protection des consommateurs organisé en juin 2000 à Bangkok, Thaïlande[13].

Constanze Picking, Directeur commerce et entreprises électroniques, Daimler Chrysler AG, présentera le document sur le règlement alternatif des litiges du dialogue mondial des entreprises sur le commerce électronique, diffusé en septembre 2000.

Louise Sylvan, Vice-Président, Consumers International, présentera un rapport récent établi par Consumers International sur les litiges dans le cyberespace. La présentation portera aussi sur les principes adoptés par le Dialogue transAtlantique avec les consommateurs en février 2000.

Session 2 : Illustration des réclamations possibles entre entreprises et consommateurs dans l'environnement en ligne

Cette session présentera des informations et des statistiques sur la nature des réclamations faites par les usagers et les consommateurs en relation avec leurs opérations et transactions en ligne. Ces informations seront présentées par les organismes de protection des consommateurs et des données et par les représentants des consommateurs afin de cerner la nature et le volume des litiges résultant des échanges et des transactions de commerce électronique entreprises-consommateurs. L'objet de cette session est de sensibiliser tous les acteurs sur les aspects qui doivent constituer les grands axes de l'étude des mécanismes de réparation et des modes alternatifs de règlement des litiges en ligne.

Présentateurs :

Michelle Childs, Chef de la politique, Association des consommateurs (*Consumers Association)* (Royaume-Uni), présentera les statistiques sur les types de réclamations reçues par la Consumers Associations et par les autres organisations de consommateurs affiliées au programme Web Trader, un partenariat regroupant des associations de consommateurs de Belgique, d'Italie, de France, des Pays-Bas, du Portugal et d'Espagne

Stephen Lau, Commissariat à la protection de la vie privée pour les données personnelles, Hong Kong, Chine, traitera de la nature des réclamations formulées par les consommateurs à Hong Kong au sujet des pratiques de traitement des données personnelles sur Internet susceptibles d'être en contravention avec les principes de protection des données énoncés dans l'ordonnance sur les données personnelles (concernant la vie privée) de Hong Kong.

Marcie Girouard, Assistante du Commissaire adjoint, Industrie Canada.

Maneesha Mithal, avocate au Bureau de la protection des consommateurs de la Federal Trade Commission (FTC) des États-Unis, présentera des statistiques sur les réclamations en ligne entre entreprises et consommateurs, reçues par leur organisme respectif. Les statistiques seront tirées principalement de Consumer Sentinel, base de données de réclamations pour fraude utilisée par les fonctionnaires chargés de l'application de la loi aux États-Unis, au Canada et en Australie. En un peu moins de cinq années de fonctionnement, la base de données renferme plus de 44 000 réclamations liées à Internet, dont un grand nombre ont une composante transnationale. Par exemple, une

réclamation sur huit reçues par les organisations américaines et canadiennes concerne des consommateurs ou des sociétés de l'étranger.

Session 3 : Règlement des litiges au stade le plus précoce – traitement interne des réclamations en ligne et remboursement des consommateurs

Dans le commerce ordinaire, le système interne des entreprises pour le traitement des réclamations est un moyen efficace de prévention et de résolution des litiges entre l'entreprise et les consommateurs. Il est prévisible que dans l'environnement en ligne, le traitement interne des réclamations sera tout aussi efficace. De même, les régimes de remboursement mis en place par le secteur des cartes de paiement peut procurer des avantages à certains consommateurs en leur assurant un remboursement : certaines de ces protections sont imposées par la loi tandis que d'autres sont assurées volontairement pour des raisons commerciales. Cette session examinera comment le traitement interne des réclamations en ligne et les remboursements pourrait résoudre les réclamations qui résultent de l'environnement en ligne entreprises-consommateurs. Elle examinera aussi le champ d'application et l'efficacité de ces mécanismes de règlement des réclamations dans l'environnement en ligne par rapport au commerce ordinaire.

Modérateur : Hugh Stevenson, Directeur adjoint, Bureau of Consumer Protection, Federal Trade Commmission (États-Unis)

Participants :

Jean Ann Fox, Directeur de la protection des consommateurs, Fédération des Consommateurs d'Amérique

Peter Møller Jensen, Responsable des relations avec l'Union européenne, Visa International

Eric Mickwitz, Médiateur finlandais pour les consommateurs

Michel Van Huffel, Direction générale de la protection de la santé et des consommateurs, Commission européenne

Présentateurs :

Charles Underhill, Directeur opérationnel par intérim, Better Business Bureau, abordera comment le code de déontologie BBB et d'autres initiatives contribuent à promouvoir l'efficacité du traitement interne des réclamations par les entreprises. Il présentera des statistiques sur les pourcentages de réussite pendant la phase de conciliation du système BBB de traitement des réclamations de tiers et les données issues de programmes analogues. La présentation mettra aussi en exergue une nouvelle initiative de BBB pour encourager le traitement interne des réclamations.

Alastair Tempest, Directeur général, Fédération du marketing direct européen (FEDMA) expliquera le rôle de la FEDMA comme organisme central pour les négociants européens, en mettant l'accent sur la façon dont le code de déontologie de la FEDMA pour le commerce électronique, le marketing interactif et les autres initiatives (« le circuit de confiance ») aide les consommateurs à obtenir réparation, notamment au-delà des frontières nationales.

Helen Bridges, Avocat, American Express Europe, présentera la politique de remboursement d'American Express et la protection des titulaires de la carte dans les transactions électroniques.

Questions suggérées :

Dispose-t-on de chiffres sur le nombre et le type de règlements obtenus par traitement des réclamations en interne et de remboursements des consommateurs par le biais des cartes de paiement ? Quelles sont les incitations susceptibles d'encourager les entreprises à traiter les réclamations en interne ? En quoi le traitement des réclamations en ligne diffère-t-il de leur traitement par téléphone, par lettre ou en personne ? Dans quelle mesure les protections en matière de remboursement sont-elles largement disponibles ? Y a-t-il d'autres mécanismes innovants qui apparaissent dans l'environnement en ligne et qui contribuent à résoudre précocement les litiges, voire à les éviter, comme les systèmes de notation/de retour d'informations, les assurances ou les dépôts fiduciaires ?

Session 4 : Modes alternatifs de règlement des litiges en ligne

Les réseaux mondiaux et le commerce électronique accroissent les possibilités d'interaction et de transaction entre individus et entreprises 24 heures sur 24, 7 jours sur 7, à très longue distance, indépendamment des frontières, des cultures locales et des systèmes juridiques. Toutefois, ces avantages mettent au défi de résoudre de façon simple et efficace d'éventuels litiges de part et d'autre, avec une garantie d'équité et de justice. L'approche pragmatique visant à offrir aux individus et aux entreprises des moyens plus accessibles et potentiellement plus efficaces de régler des litiges qui, autrement, ne pourraient pas l'être facilement offre une solution intéressante.

La présente session examinera, à travers la présentation des modes alternatifs de règlement des litiges, déjà existants ou en cours de développement, la grande diversité des approches possibles pour régler les litiges qui surviennent en ligne. Afin d'attirer l'attention sur les éléments spécifiques, procéduraux et autres, de ces divers mécanismes et de faciliter les débats du 2^{e} jour, on procédera en trois parties. Le premier débat est consacré aux mécanismes entièrement automatisés dont les résultats sont obtenus sans intervention de l'homme. Le deuxième et le troisième débats examineront les autres mécanismes, d'un formalisme variable sur le plan de la procédure et faisant plus ou moins intervenir un tiers neutre. Enfin, le quatrième débat, en explorant les systèmes en cours de développement, portera sur les objectifs et la méthodologie nécessaire pour mettre en place un mécanisme alternatif de règlement des litiges en ligne.

***Modérateur* :** Bernard Clements, Chef de service, Centre de recherche commun, Commission européenne.

Participants :

John Borking, Membre du Commissariat à la vie privée des Pays-Bas

Dana Haviland, Associé, Wilson Sonsini Goodrich & Rosati

Ethan Katsh, Directeur, Centre pour les technologies de l'information et le règlement des litiges, Université du Massachusetts

Pippa Lawson, Avocat, Centre de défense des intérêts du public

Odile Nicholas-Etienne, Union Fédérale des Consommateurs

Charles Underhill, Directeur opérationnel par intérim, Better Business Bureau.

I. Mécanismes entièrement automatisés de règlement des litiges en ligne

(par exemple, résultat généré par ordinateur)

La plupart des systèmes automatiques de règlement alternatif des litiges sont destinés à résoudre les litiges pécuniaires, notamment en matière d'assurance, et supposent que les parties, avant d'entrer en négociation, conviennent de se conformer à la solution si le litige se règle. Toutefois, il existe un petit nombre de programmes automatiques qui permettent aux parties de choisir au départ d'être ou non tenues par la solution du différend[14]. La présente session examinera si ces systèmes peuvent contribuer à régler les litiges entre entreprises et consommateurs dans le domaine de la protection des consommateurs et de la vie privée.

Présentateur :

Richard Belczynski, Vice-Président, Division internationale et commerciale, ClickNSettle, présentera le système de ClickNSettle, qui génère automatiquement le règlement par ordinateur. La présentation portera aussi sur la nature des litiges qui peuvent être ou ont été réglés par ClickNSettle et la répartition géographique des parties qui ont recouru au système ClickNSettle.

II. Mécanismes de règlement souples

(par exemple, négociation/médiation)

Présentateurs :

Colin Rule, Directeur général de Online Resolution, Inc., décrira dans les grandes lignes les différentes méthodes de règlement des litiges de onlineresolution.com en insistant tout particulièrement sur son outil de collaboration en ligne, Resolution Room. Il s'agit d'un environnement interactif qui regroupe des forums de discussion, des forums de consultation privés, un outil de vote et une fonction calendrier que le tiers neutre peut configurer pour l'adapter au mieux aux besoins des parties. (www.onlineresolution.com)

Cara Cherry Lisco, Directeur du réseau de règlement des litiges en ligne de SquareTrade, présentera un outil en ligne modulaire et un service de règlement des litiges, mis en place en février 2000. Elle montrera comment SquareTrade a été efficacement introduit comme mécanisme de recours neutre dans presque 2 millions de transactions par semaine et constitue le prestataire préféré de règlement des litiges pour les utilisateurs d'eBay[15]. Elle commentera également les enseignements tirés de son expérience dans le traitement de plus de 17 000 litiges dans plus de 80 pays, en plusieurs langues dont l'anglais, l'allemand et l'espagnol.

III. Mécanismes de règlement formels

(par exemple, médiation/arbitrage)

Présentateurs :

Erik Wilbers Avocat principal du Centre de médiation et d'arbitrage de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) présentera des conclusions pratiques tirées de l'expérience en la

matière du centre de médiation et d'arbitrage de l'OMPI, qui peuvent être intéressantes pour élaborer de bonnes méthodes de résolution des litiges de consommation. Ces dernières années, ce centre a acquis une certaine expérience dans la conception et l'application des procédures en ligne de règlement des litiges. Ce centre a administré en ligne plus de 1600 litiges concernant des noms de domaines. Il a également travaillé au développement d'applications plus génériques destinées à l'arbitrage de tous types de litiges conformément aux règles de l'OMPI. (www.wipo.org)

Fabien Gélinas, Vice-Président et Directeur juridique de e-Resolution, présentera le système d'arbitrage en ligne de l'entreprise pour les noms de domaine et les autres différends. Il étudiera la procédure d'arbitrage entre entreprises et consommateurs et fera quelques comparaisons avec le règlement des litiges en ligne entre entreprises et consommateurs. La présentation abordera aussi les questions d'exécution de la décision arbitrale et de l'applicabilité de l'arbitrage au règlement des litiges entre entreprises et consommateurs en fonction de l'expérience d'eResolution. (www.eresolution.com)

IV. Modes alternatifs de règlement des litiges en cours de développement

Présentateurs :

Duncan McDonald, Institut américain d'études allemandes contemporaines (AICGS), présentera la proposition de son institut consistant à créer un réseau d'universités américaines et européennes pour servir de médiateur afin de faire face à la confusion des consommateurs en ce qui concerne la gestion des litiges, les prestataires de modes de règlement alternatif des litiges et les droits prévus par la loi. L'accent sera mis sur la grande diversité des questions juridiques et autres qui doivent absolument être réglées pour instaurer et mettre en œuvre un système transfrontière efficace.

Vincent Tilman, Chercheur, Centre de Recherches Informatique et Droit (CRID) décrira ECODIR, projet de règlement alternatif des litiges transnationaux actuellement en cours de développement. Le projet, subventionné par l'Union européenne, vise à fournir aux consommateurs un système d'aide pour l'arbitrage et la médiation en ligne afin de régler les litiges résultant de l'utilisation d'Internet. Le projet est dirigé par le CRID, Université de Namur, en collaboration avec un consortium d'universités, de centres de médiation et de partenaires du secteur privé d'Europe et d'Amérique du Nord. La présentation mettra en exergue les objectifs, la méthodologie et le plan de développement d'ECODIR et traitera notamment des défis à relever dans la mise en place d'un système de ce type dans un environnement multilingue transnational.

Christopher Kuner, Avocat, Morrison & Foerster, LLC, présentera la politique future de la Chambre de Commerce Internationale (CCI) pour le règlement alternatif des litiges entre entreprises et consommateurs dans le commerce électronique. La présentation s'appuiera sur un document d'orientation, en cours de formulation par la CCI, sur le règlement alternatif des litiges dans les transactions entre entreprises et consommateurs. Ce document est destiné à déterminer certains des principes saillants dont la CCI pense qu'ils devraient régir ce domaine et à donner un aperçu des mesures concrètes qu'elle devrait prendre.

Questions suggérées :

Quelle est l'expérience des utilisateurs et des consommateurs en ce qui concerne le règlement alternatif des litiges ? Y a-t-il des types particuliers de litiges qui ne se prêtent pas à une résolution par un mode de règlement alternatif des litiges en ligne ? Y a-t-il des catégories de litige qui seraient

mieux réglées par un type précis de règlement alternatif des litiges en ligne ? D'autres questions pourront porter sur les appendices 1 et 2 (liste des modes alternatifs de règlement des litiges en ligne et liste des éléments procéduraux et substantiels qui existent dans les mécanismes alternatifs de règlement des litiges).

Deuxième jour : mise en place de mécanismes alternatifs efficaces de règlement des litiges en ligne au niveau mondial

Sur la base des exposés de la première journée, le débat se concentrera sur les différents défis à relever pour favoriser le recours aux modes alternatifs de règlement des litiges entre entreprises et consommateurs à l'échelon national et mondial, sur les aspects incitant les entreprises, les consommateurs et les pouvoirs publics à participer et/ou à encourager l'utilisation de ces mécanismes, ainsi que sur les facteurs dissuasifs. La session 5 s'intéressera aux problèmes posés par le règlement des différends en ligne : il s'agira notamment d'identifier les éléments importants assurant l'équité et l'efficacité des mécanismes en ligne. La session 6 s'attachera au rôle que doivent jouer les acteurs pour promouvoir ces deux principes, en assurer le respect et la mise en œuvre et sensibiliser l'ensemble des acteurs.

Allocution d'ouverture par la Présidente de la 2ème journée

Jytte Ølgaard, Présidente, Comité de la politique à l'égard des consommateurs de l'OCDE

Session 5 : Les défis posés à relever pour le règlement des litiges en ligne

Tout le monde est conscient des obstacles potentiels, notamment juridiques, que soulève le recours aux tribunaux dans les différends découlant d'interactions transfrontières en ligne : quel est le droit applicable, quelle instance est compétente pour ce différend, quelle juridiction est compétente pour connaître de ce litige, la décision peut-elle être exécutée à l'étranger ? Une autre préoccupation légitime, même si elle est de nature moins juridique, concerne le coût des procédures judiciaires, qui peut dépasser la valeur des biens et des services objets du litige, ou la durée de la procédure, qui est généralement beaucoup plus longue que dans le monde virtuel.

Cette session étudiera et débattra de la diversité des défis possibles que posent l'utilisation et la mise en œuvre efficaces des modes alternatifs de règlement des litiges (RAL) en ligne, au niveau socio-économique (notamment sur les plans linguistique et culturel), juridique (notamment le principe du recours en dernier ressort) et technologique (notamment la sécurité). Tout en discutant de ces défis, les participants pourront reconnaître la nécessité de trouver un terrain d'entente entre les acteurs sur des éléments essentiels qui doivent être inclus dans tout RAL en ligne équitable et efficace pour les différends entre entreprises et consommateurs, dont *i)* la transparence, c'est-à-dire que les informations sur les RAL, leur coût et d'autres aspects importants doivent être directement accessibles à tous les acteurs avant que soit engagée une procédure RAL ; *ii)* l'accessibilité ; i*ii)* la gratuité ou un coût modéré pour le consommateur et *iv)* la rapidité des décisions.

I. Questions socio-économiques liées aux RAL en ligne

« Derrière les écrans se trouvent des personnes de toutes nationalités, de tous groupes ethniques et culturels, de toutes classes sociales et professionnelles, de toutes religions et convictions politiques, de tous âges et styles de vie, des deux sexes, qui, ensemble, mais aussi entre elles, montrent la vaste diversité des préférences et des aversions, des espoirs et des craintes pour l'avenir, des goûts et des dégoûts[16]». Cette citation illustre bien la complexité de l'environnement en ligne mondial dans sa dimension sociologique, notamment en ce qui concerne les interactions entre les entreprises et les consommateurs. De même que les questions juridiques et techniques, il faut analyser les facteurs sociologiques et économiques afin de mieux comprendre quelle influence ils peuvent exercer sur l'utilisation et la mise en œuvre des RAL en ligne.

Cette session s'intéressera à certains des défis socio-économiques, notamment à l'impact des différences culturelles, linguistiques et économiques sur l'efficacité des RAL, ou, de même, à l'impact des différences d'information et d'expertise sur l'utilisation et la mise en œuvre des RAL, en considérant que les outils de communication en ligne (numérisation des textes, des sons, des images fixes ou vidéo) influencent les méthodes de travail, les schémas culturels et les styles de vie[17].

Modératrice : Anna Fielder, directeur, Consumers International

Participants :

Giles Buckenham, administrateur, Direction générale de la santé et de la protection des consommateurs, Commission européenne

Scott Cooper, directeur, politique des technologies, Hewlett-Packard

Carmen Fernandez Neira, présidente, groupe de travail Internet, European Advertising Standards Alliance (EASA)

William Marsh, directeur, CEDR

Toh See Kiat, associé, Tan Peng Chin and Partners

Présentateurs :

Nora Femenia, professeur et présidente d'Inter-Mediacion, Inc., analysera comment les modes de règlement des différends en ligne et la gestion des réclamations des consommateurs au niveau mondial pourraient répondre aux différents environnements sociaux et culturels. Elle s'attachera aux approches culturelles différentes qui sous-tendent les réclamations des usagers, à l'impact de la pression de la collectivité pour le règlement des différends et au rôle que devraient jouer les techniques de négociation assistée par ordinateur pour sensibiliser le public aux moyens légitimes de résoudre les problèmes liés aux transactions en ligne.

Christopher Drahozal, professeur à l'University of Kansas School of Law, analysera sous un angle économique diverses questions liées à l'équité des RAL en ligne, en tentant notamment de répondre aux interrogations suivantes : pourquoi les parties ont-elles recours aux RAL ? Les RAL remplacent-ils les actions en justice ? Quel est l'impact des incitations des acteurs et du tiers neutre sur l'utilisation et la mise en œuvre des RAL ? En quoi les différences au niveau des ressources et des informations entre les entreprises et les consommateurs peuvent-elles susciter des inquiétudes quant au caractère équitable des RAL en ligne ?

Questions suggérées :

Quelle est l'incidence des différences linguistiques et culturelles sur l'utilisation et la mise en œuvre des RAL ? Faut-il offrir aux utilisateurs et aux consommateurs la possibilité d'interagir dans leur propre langue pendant la procédure RAL ? Quel est l'impact des différences économiques sur l'utilisation et la mise en œuvre des RAL ? Existe-t-il un moyen de gommer les déséquilibres au niveau de l'information et de l'expertise dont disposent les parties ? La formation des tiers neutres doit-elle inclure les aspects socio-économiques ?

II. Questions juridiques liées aux RAL en ligne

Les questions juridiques ont trait aux éléments qui visent à rendre la procédure RAL équitable et efficace tant pour les consommateurs que pour les entreprises. Cette session soulignera les aspects procéduraux et substantiels considérés comme essentiels pour garantir une procédure équitable et efficace, tout en reconnaissant qu'ils sont susceptibles de varier selon le type de RAL et/ou de différend.

Au cours de la discussion, les participants reconnaîtront sans doute la nécessité de trouver un terrain d'entente notamment sur les points suivants *i)* l'indépendance des prestataires de RAL pour les différends en ligne entre entreprises et consommateurs ; *ii)* la neutralité ou l'impartialité des décisions des intermédiaires dans la procédure RAL, et la question de savoir s'ils disposent des compétences et de la formation nécessaires pour remplir convenablement leur mission ; *iii)* les consommateurs doivent-ils être autorisés à choisir entre les RAL et les mécanismes juridiques traditionnels, autrement dit le recours aux RAL doit-il se faire sur une base volontaire ou obligatoire ? *iv)* la question de la représentation ou non des parties ou 5) la procédure doit-elle être contradictoire ?

Parmi les autres questions à débattre, il faut se demander si les systèmes juridiques actuels empêchent les consommateurs de recourir aux RAL ou les entreprises de mettre en œuvre des décisions, rendues au titre des RAL, avec lesquelles les consommateurs sont entièrement d'accord. Outre les questions plus procédurales, il convient d'examiner un aspect important : les principes de fond qu'il faut appliquer pour résoudre un différend transfrontière en ligne[18].

On pourra également se demander si la décision rendue à l'issue d'une procédure RAL doit ou non avoir un caractère obligatoire. Même s'il s'agit là d'un thème important, il sera rappelé aux participants que la Conférence se concentre en premier lieu sur les RAL les plus flexibles et les plus informels.

Modératrice : Mozelle Thompson, commissaire, US Federal Trade Commission

Participants :

Matthias Blume, ministère de la justice, Autriche

Eric Ducoulombier, administrateur, Direction générale du marché intérieur, Commission européenne

Marco Gasparinetti, Commission pour la protection des données, Italie

Michael Geist, professeur, University of Ottawa Law School

James Murray, directeur, Bureau Européen des Unions de Consommateurs

Ron Plesser, associé, Piper Marbury Rudnick & Wolfe, et coordinateur, Commerce électronique et groupe de protection des consommateurs

Présentateurs :

Philippe Fouchard, professeur, Université de Paris II, examinera les principaux éléments juridiques nécessaires pour que les RAL soient équitables et efficaces pour les utilisateurs et pour les consommateurs. Il s'intéressera particulièrement aux cas où les parties sont d'accord avec l'application du RAL et acceptent le règlement à l'issue de la procédure.

Christopher Kuner, Cabinet de consultants Morrison & Foerster, LLC, présentera une vue d'ensemble des principales conclusions d'une étude sur les obstacles juridiques à l'utilisation des RAL dans les transactions de commerce électronique entre entreprises et consommateurs en Europe. Cette étude a été demandée au printemps dernier par le Dialogue mondial des entreprises sur le commerce électronique, face aux incertitudes et à la confusion suscitées par le cadre juridique des RAL entre entreprises et consommateurs en Europe.

Questions suggérées :

Comment le droit national ou international et les questions connexes de politique publique peuvent-ils avoir une incidence sur l'utilisation ou la mise en œuvre des RAL (par exemple, les droits inaliénables, les différences dans le droit substantiel ou les règles procédurales liées aux RAL) ? Quel est l'impact du droit sur les possibilités de règlement extrajudiciaire des différends ?

III. Principe de la décision en dernier ressort et juge d'appui

Cette session se concentrera sur l'interface entre les RAL en ligne et le cadre juridictionnel.

On s'attend à ce que les systèmes internes de traitement des réclamations des entreprises et les mécanismes RAL en ligne soient à même résoudre la plupart des différends provenant des interactions en ligne entre entreprises et consommateurs. Cependant, dans les cas où les mécanismes alternatifs échouent, il peut s'avérer nécessaire de recourir aux tribunaux. En outre, comme pour l'arbitrage, le recours à un juge (juge d'appui)[19] au cours d'une procédure RAL peut contribuer à lever une difficulté (par exemple, si le prestataire de services cesse ses activités pendant la procédure, ou s'il y a une violation grave des principes d'indépendance et d'impartialité) ou à faciliter le bon fonctionnement et l'aboutissement d'une procédure. La discussion comprendra une étude approfondie de l'applicabilité des notions traditionnelles de juridiction compétente et des questions d'exécution ainsi qu'une analyse des solutions existantes et des propositions de solutions nouvelles. Elle s'attachera également à étudier la possibilité pratique d'adapter le concept de juge d'appui aux procédures RAL en ligne les moins formelles.

Modératrice : Catherine Kessedjian, professeur, Université de Paris II, ex Secrétaire générale adjointe de la Conférence de la Haye de droit international privé

Participants :

Katharina Boele-Woelki, professeur, Université d'Utrecht

Giacinto Bisogni, Expert national aux services juridiques de la Commission européenne

Asunción Caparrós, directeur, Affaires européennes, ABN Amro Bank

Roger Cochetti, Senior Vice President et Chief Policy Officer, Network Solutions

David Goddard, avocat, Commissariat du droit néo-zélandais

Pippa Lawson, avocat conseil, Public Interest Advocacy Centre

IV. Problèmes technologiques liés aux RAL en ligne et évolutions actuelles

L'évolution actuelle des applications technologiques et des pratiques, ainsi que l'interopérabilité croissante des systèmes, ont un impact sur le développement des RAL en ligne. Il est par conséquent important de débattre de l'innovation technologique continue sur Internet en relation avec les RAL en ligne. Cette session mettra en évidence les technologies déjà utilisées ou en cours d'élaboration afin de montrer comment elles peuvent contribuer à faciliter le règlement de différends en ligne entre les entreprises et les consommateurs. Ainsi, les technologies servant à protéger la signature et l'authentification électroniques[20], ou le chiffrement des messages, peuvent contribuer à assurer la confidentialité et l'intégrité de la procédure et de l'information échangée. Par ailleurs, grâce aux technologies interactives, telles que la vidéoconférence, les parties peuvent se rassembler en un même lieu virtuel, au lieu de rester derrière leur écran informatique, et l'interaction se fait face-à-face. De même, la traduction automatique et la reconnaissance vocale permettent de surmonter certaines différences culturelles.

Au cours de la discussion, les participants pourront également examiner la nécessité de trouver un terrain d'entente sur des questions liées à la sécurité des RAL en ligne ainsi qu'à la confidentialité et à l'intégrité de la procédure et de l'information échangée.

Modérateur : Wibo Koole, Chef du département de la politique à l'égard des consommateurs, Consumentenbond

Participants :

Sarah Andrews, Policy Analyst, EPIC/Privacy International

Peter Lübkert, Technologies de l'information et des réseaux, OCDE

Marc Wilikens, Centre de recherche mixte, Commission européenne

Présentateurs :

Joseph Alhadeff, vice-président, Politique publique mondiale, Oracle, exposera les aspects stratégiques des questions et des défis technologiques en termes d'efficacité des RAL en ligne dans le règlement des différends entre entreprises et consommateurs.

Chris Lynn, Avocat conseil, Microsoft Europe, Afrique et Moyen-Orient, présentera les progrès réalisés au niveau des logiciels pour accroître l'efficacité des mécanismes de règlement des différends simples entre entreprises et consommateurs.

Questions suggérées :

Comment l'innovation technologique permettra-t-elle de relever ces défis ? Comment garantir l'interopérabilité technologique ? L'innovation technologique peut-elle gommer les différences culturelles et autres différences sociologiques entre les parties ?

Session 6 : Le rôle des acteurs

La plupart des acteurs admettent que les modes alternatifs de règlement des litiges en ligne (RAL) peuvent être très utiles aux deux parties à une interaction ou une transaction électronique, particulièrement dans le cas des litiges transnationaux. Ils considèrent qu'il existe des incitations à recourir aux RAL, que ce soit pour des raisons économiques (réduction des coûts), juridiques (pour contribuer à résoudre la question très complexe de la juridiction compétente, car avec le règlement des litiges en ligne, la juridiction ne sera plus déterminée par des critères géographiques, et sera d'ordre virtuel) ou plus sociologiques (par exemple pour renforcer la confiance et compenser les différences culturelles). D'éventuels effets négatifs ont également été exposés, tels que l'absence de choix pour le consommateur, les disparités entre les parties (comme le manque d'information, d'instruction et de moyens) ou le risque qu'il soit impossible de faire exécuter la décision.

A partir des discussions précédentes, cette dernière session est destinée à mettre en évidence l'opinion partagée par les acteurs sur un certain nombre d'éléments socio-économiques, juridiques ou technologiques que devrait comporter tout RAL en ligne équitable et efficace pour les litiges entre entreprises et consommateurs. Les participants se demanderont aussi quel est le meilleur moyen de favoriser leur mise en œuvre, en explorant deux grands domaines d'action possibles.

Cette session sera donc subdivisée en deux débats. Le premier sera consacré au rôle des acteurs dans la promotion des éléments essentiels des RAL en ligne (réglementation, auto-régulation ou approche intégrée) et la garantie de la conformité (programmes de labels destinés aux secteurs public et privé). Le deuxième portera sur les mesures de sensibilisation et d'information du public sur les RAL.

Cette session a pour but d'insister sur la nécessité que les acteurs adoptent des approches complémentaires pour équilibrer efficacement les intérêts des individus et des entreprises, tout en exploitant le savoir-faire de tel ou tel acteur, le cas échéant.

Modérateur : Arie J. M. van Bellen, Directeur exécutif, Electronic Commerce Platform Nederland

Participants :

Roger Cochetti, Senior Vice president et Chief Policy Officer, Network Solutions

Susan Grant, directeur du centre national d'information sur la fraude (Director of National Fraud Information Center), Ligue nationale des consommateurs (National Consumer League)

David Mair, administrateur, direction générale de la santé et de la protection des consommateurs, Commission européenne

Rebecca Richards, directeur politique et harmonisation, TRUSTe

Yuko Yasunaga, directeur adjoint, division de la politique commerciale, MITI, Japon

I. Promouvoir la loyauté et l'efficacité des RAL en ligne et assurer la bonne mise en œuvre (par exemple programmes de labellisation/certification)

Comme nous l'avons vu lors de la session 1, divers acteurs ont élaboré des principes pour les systèmes RAL entre entreprises et consommateurs ou exprimé leur opinion sur des éléments essentiels de ces systèmes. Cette session étudiera le rôle des acteurs dans la promotion des RAL entreprises-consommateurs en ligne équitables et efficaces. Les participants se demanderont comment les acteurs devraient coopérer pour identifier les éléments essentiels des RAL en ligne (par exemple : Qui doit siéger ? Les différents acteurs doivent-ils formuler des recommandations différentes, comme c'est actuellement le cas ? Sur quelles règles se fonder pour les RAL, une réglementation ou des codes de conduite ?). Ils chercheront également à savoir comment les acteurs peuvent œuvrer ensemble au respect de ces éléments.

Parmi les autres mesures complémentaires, il convient d'étudier les programmes de certification et de labellisation, qui peuvent influer positivement sur la question de la conformité, et qui impliquent des approches pouvant être envisagées à la fois par le secteur privé et les pouvoirs publics. Les acteurs ont engagé une discussion pour savoir si et comment ces programmes doivent être conçus pour assurer l'équité et l'efficacité des systèmes RAL en ligne, comment vérifier la conformité à ces programmes et comment faire appliquer les décisions rendues par les systèmes RAL en ligne dans le cadre de ces programmes.

Présentateurs :

Naoshi Shima, vice-présidente, Business Development, NEC, exposera comment le dialogue mondial des entreprises sur le commerce électronique a coordonné avec succès ses récentes recommandations sur les RAL entre entreprises et consommateurs. En qualité de principal organisateur des travaux du dialogue dans la région Asie/Océanie, au nom de NEC, Mme Shima se penchera sur l'expérience asiatique concernant le règlement des différends en ligne entre les consommateurs et les entreprises.

Barbara Wellbery, associée, Morrison & Foerster LLC, décrira la méthode mise en œuvre aux États-Unis pour favoriser la confiance entre les consommateurs et les entreprises dans le commerce électronique en ce qui concerne la protection de la vie privée et du consommateur, en se concentrant sur les RAL en ligne. La méthode américaine comprend un ensemble complémentaire de mécanismes mis en œuvre par les divers secteurs, d'initiatives gouvernementales et de mesures visant d'application des lois. Elle décrira par ailleurs le système d'auto-régulation en vigueur dans son pays concernant les transactions commerciales et la protection de la vie privée.

Martin Bond, assistant du directeur, ministère britannique du commerce et de l'industrie (*Department of Trade and Industry*), Royaume-Uni, expliquera comment les pouvoirs publics, les entreprises et les organisations de consommateurs britanniques en sont venus à développer conjointement le programme TrustUK. Il indiquera comment ce programme a été élaboré, comment il fonctionne et à quel niveau les RAL s'intègrent dans le système.

Malcolm Crompton, commissaire pour la protection des données, Australie, s'intéressera aux programmes de labellisation en ligne. Il présentera les conclusions d'une étude sur les Programmes en ligne de protection de la vie privée réalisée en septembre conjointement par son bureau et celui du Commissaire à la protection de l'information et de la vie privée de l'Ontario. Ce travail a permis de mettre en évidence trois composants essentiels d'un programme de labellisation, à savoir des principes de protection de la vie privée suffisamment puissants, une bonne méthode de résolution des litiges et un mécanisme de mise en application efficace.

Questions suggérées :

Est-il souhaitable que les acteurs convergent dans la définition des éléments essentiels pour la promotion de RAL en ligne équitables et efficaces ? Quels doivent être les acteurs participants ? Quel est le rôle des acteurs dans l'élaboration des programmes de labels et des codes de conduite, la mise au point de systèmes de recours communs et l'application des décisions ? Comment les acteurs peuvent-ils coopérer au mieux pour développer ces programmes et les systèmes de transaction transfrontières ?

II. Éducation des entreprises, des consommateurs et des administrations publiques dans le domaine des RAL en ligne

Les RAL transnationaux sont monnaie courante d'entreprise à entreprise, mais c'est un phénomène nouveau entre entreprises et consommateurs. On attend des RAL en ligne qu'ils règlent efficacement les litiges dans le monde virtuel, mais il faut admettre que les utilisateurs et les consommateurs connaissent et comprennent mal ces systèmes. Conscients de ce besoin d'information, les participants à cette session se concentreront sur le rôle des divers acteurs dans la sensibilisation des entreprises et des consommateurs. La discussion portera sur les moyens permettant de sensibiliser efficacement les entreprises aux possibilités qu'offrent les RAL et de renseigner les consommateurs sur la nature des RAL équitables et efficaces et sur les procédures y afférentes.

Présentateurs :

Duncan McDonald, Institut américain d'études allemandes contemporaines, expliquera comment la transparence, via des communications en ligne claires, en termes simples et en plusieurs langues, peut minimiser la confusion et la méfiance du consommateur, la mauvaise impression véhiculée par les médias et l'attention et l'intervention des pouvoirs publics.

Francis Aldhouse, adjoint au commissaire pour la protection des données, Royaume-Uni, indiquera comment le commissaire britannique chargé de la protection des données soutient les systèmes de garantie de service à la clientèle, d'intervention d'un médiateur, de règlement des litiges sectoriels et d'autres exemples de RAL et utilise la publicité formelle et les techniques de RP pour informer les individus de leurs droits et les encourager à les faire valoir et à exiger la protection de leur vie privée.

Questions suggérées :

Quel est le rôle des acteurs dans l'information des entreprises, des consommateurs et des pouvoirs publics sur les RAL en ligne ? Que peuvent faire les acteurs pour assurer la participation de tous aux RAL ? Quels sont les facteurs qui incitent les différents acteurs à promouvoir les RAL en ligne et ceux qui les en dissuadent ?

Conclusion de la conférence

La conférence se conclura sur un bref récapitulatif des temps forts des débats.

Compte rendu de la conférence

Principaux points

Les différents acteurs doivent coopérer étroitement, et les mécanismes de règlement alternatif des litiges doivent être souples

L'Internet est mondial et sans frontière. Dans la conception de mécanismes de règlement alternatif des litiges en ligne, il convient de prendre en considération les points de vue de toutes les parties prenantes, aussi bien administrations publiques qu'entreprises ou groupes de consommateurs. A cet égard, un principe cardinal des mécanismes de règlement alternatif des litiges en ligne, quels qu'ils soient, doit être la flexibilité, pour qu'ils puissent tenir compte des différences entre pays et culture et faire face à la diversité des litiges qui peuvent surgir. Le RAL peut être une voie de recours juste et efficace pour les utilisateurs dans l'environnement en ligne. De façon plus générale, des mécanismes de RAL en ligne efficaces peuvent contribuer à renforcer le sentiment de confiance entre les entreprises, les utilisateurs et les consommateurs sur Internet, lequel est indispensable que le commerce électronique poursuive son essor.

Des éléments communs ont été dégagés pour les principes du règlement alternatif des litiges

Il n'y a pas de solution unique en matière de RAL et différents contextes (en valeur ou en complexité, par exemple) peuvent nécessiter des approches différentes. Dans le même temps, certains principes communs entre les autorités publiques, les industries et les groupes de consommateurs sont apparus s'agissant de définir des mécanismes de règlement alternatif des litiges équitables et efficaces, notamment accessibilité, modicité du coût pour les consommateurs, transparence (c'est-à-dire la fourniture aux consommateurs des informations indispensables pour qu'ils puissent choisir en connaissance de cause un mécanisme de règlement alternatif), rapidité des décisions, prise en compte des diversités culturelles et linguistiques dans la procédure de RAL, et recours à des intermédiaires impartiaux et qualifiés pour la conduite du RAL.

Des différences sont apparues

Trois domaines sont apparus clairement sur lesquels le débat doit être poursuivi entre les parties prenantes. Tout d'abord, les acteurs divergent sur la question de savoir s'il existe des situations dans lesquelles les consommateurs devraient avoir l'obligation d'engager une procédure de RAL, avant une action en justice. Deuxièmement, les avis divergent aussi sur le fait de savoir si les règlements issus d'une procédure de RAL en ligne devraient, ou même pourraient, s'imposer aux parties. Troisièmement, les parties prenantes doivent examiner de façon plus approfondie quels sont les moyens les plus efficaces d'assurer le respect et l'exécution des procédures et décisions de RAL.

Les réclamations d'utilisateurs et de consommateurs se multiplient dans le secteur du commerce électronique

Le nombre de réclamations liées au respect de la vie privée et à la protection du consommateur dans le cadre d'Internet augmente chaque année. Les plus fréquentes concernant la protection des consommateurs dans le commerce électronique portent sur le fait que les marchandises n'ont pas été livrées à temps ou même ne l'ont pas été du tout, que des frais et coûts n'étaient pas signalés, que

l'information concernant les produits était insuffisante et que les réclamations sont traitées de façon inadéquate. Celles concernant le respect de la vie privé portent principalement sur le recueil de données sans le consentement de l'intéressé, l'utilisation des données à des fins autres que celles pour lesquelles elles ont été au départ recueillies, la vente de données à des tiers, l'envoi de courriers électroniques commerciaux non sollicités, l'usurpation d'identité, la fourniture d'informations sur la solvabilité sans le consentement de l'intéressé et la protection de la vie privée des enfants en ligne. Les réclamations de consommateurs d'un pays à l'encontre de commerçants situés à l'étranger commencent tout juste à apparaître.

Le consensus général est que les litiges devraient être réglés le plus rapidement possible

Les litiges internationaux entre entreprises et consommateurs devraient être réglés le plus rapidement possible, dans l'intérêt de toutes les parties. La première mesure pour la solution des litiges en ligne est de les éviter. A cet effet, les entreprises devraient mettre en place des systèmes efficaces et efficients de services clients et de traitement interne des réclamations. Les mécanismes de remboursement des clients et autres systèmes analogues sont également utiles, même s'ils sont de portée limitée. De manière générale, les clients en ligne sont très exigeants concernant les temps de réponse des entreprises en ligne. Des systèmes efficaces et rapides de traitement des réclamations des clients renforcent de façon spectaculaire la loyauté de la clientèle.

Tout comme pour les réclamations concernant une possible fraude le règlement alternatif peut être inadapté, tous les programmes de RAL en ligne peuvent ne pas convenir à l'ensemble des litiges liés au respect de la vie privée et à la protection des consommateurs

Il existe tout un éventail de programmes de RAL en ligne, depuis ceux entièrement automatisés jusqu'aux systèmes qui, à l'autre extrémité, reposent sur un processus formel d'arbitrage. Entre ces deux extrêmes, il existe toute une variété de systèmes qui présentent chacun des avantages et des inconvénients pour les clients comme pour les entreprises. Si tous les mécanismes ne sont pas adaptés à tous les litiges, l'élaboration d'un large éventail de mécanismes peut aider à apporter une réponse à la grande diversité des litiges ; une saine concurrence entre ces mécanismes est souhaitable. Des conseils pratiques et une information suffisante sont nécessaires pour que les parties puissent choisir le mécanisme de RAL le mieux adapté à chaque cas.

Des obstacles socio-économiques et culturels subsistent

Il faut que les fournisseurs de systèmes de RAL et de services connexes s'attachent à rendre les mécanismes de ce type de véritablement accessibles à tous. De nombreux obstacles socio-économiques et culturels freinent la mise en place de systèmes équitables et efficaces pour le règlement alternatif des litiges en ligne à l'échelle internationale. Les barrières linguistiques sont notamment un problème fréquent, tout comme les différences culturelles dans l'approche des litiges et des désaccords. Il importe que les fournisseurs de systèmes de RAL soient conscients de ces problèmes et qu'ils s'attachent à y apporter des solutions.

La technologie peut favoriser le RAL en ligne, mais elle présente également un paradoxe

Des progrès dans des domaines comme les langages informatiques, la vidéoconférence enrichie, la traduction, la reconnaissance vocale et l'accès à large bande peuvent faciliter le développement des mécanismes de RAL en ligne et amener les parties dans une relation quasi-équivalente à un face à face. Toutefois, dans les cas où des mécanismes de résolution des litiges synchrones (notamment en face à face) peuvent sembler préférables à certains utilisateurs, une communication asynchrone peut donner à l'une des parties l'avantage d'un délai de délibération plus long avant une réponse.

Le débat se poursuit sur les rôles possibles des juges pendant la procédure de RAL, de même qu'en dernier ressort

Lors de la conférence, on a examiné quatre situations concernant l'intervention des autorités judiciaires dans le contexte du RAL : *i)* comme autorité pour faire appliquer une décision, puisque les tribunaux ont l'exercice exclusif des pouvoirs de contrainte ; *ii)* comme juge en dernier ressort ; *iii)* comme *juge d'appui*, en cas d'arbitrage contraignant et *iv)* pour faire appliquer un accord de règlement. Il semble qu'il y ait peu de partisans de l'intervention d'un juge (*juge d'appui*) dans une procédure de RAL en ligne de type non arbitral, car cela pourrait remettre en cause le principe d'une procédure informelle et rendre celle-ci coûteuse pour les deux parties.

Le moment est peut-être venu pour les différentes parties d'unir leurs forces

Toutes les parties ont de façon indépendante énoncé des principes, recommandations et orientations concernant le RAL. S'il subsiste des points de divergence, les domaines d'entente sont nombreux. Il existe un accord sur le fait que les différents acteurs devraient œuvrer ensemble pour s'entendre sur davantage de principes pour assurer l'application de mécanismes de RAL justes et efficaces aux litiges liés à la protection de la vie privée et la consommation dans le contexte du commerce électronique entre entreprises et consommateurs.

Premier jour : Panorama des modes alternatifs de règlement des litiges en relation avec l'environnement en ligne

La conférence est ouverte par M. Peter Ford, Président du Groupe de travail sur la sécurité de l'information et la vie privée de l'OCDE et Mme Jytte Ølgaard, Présidente du Comité de la politique à l'égard des consommateurs de l'OCDE.

Accueil et allocution liminaire

M. A.H. Korthals**,** Ministre de la Justice des Pays-Bas, évoque le commerce électronique en général et rappelle ensuite qu'il existe une divergence fondamentale entre le caractère national des gouvernements et de leurs systèmes juridiques et la nature sans frontière de l'Internet. M. Korthals propose aux participants d'examiner quatre questions : *i)* à quel niveau et sous quelle forme la réglementation devrait-elle intervenir ? ; *ii)* les mêmes normes et les mêmes valeurs devraient-elles s'appliquer en ligne et hors ligne ? ; *iii)* est-il possible de définir clairement quels aspects du droit international privé interviennent ? ; *iv)* comment appliquer les lois dans un monde sans frontières ? Il souligne que le RAL a pour avantage de résoudre de manière rapide et efficace les litiges en

surmontant le problème de la compétence judiciaire et suggère qu'un système de médiation numérique, un moyen par lequel les deux parties s'engagent de plein gré à respecter la décision prise à l'issue de la procédure, constitue peut-être la meilleure solution.

M. Herwig Schlögl, Secrétaire général adjoint de l'OCDE, fait remarquer que cette importante conférence internationale est la première de son genre à évoquer les problèmes de règlement alternatif des litiges en ligne et, conformément à la pratique de l'OCDE, à réunir toutes les parties prenantes. M. Schlögl rappelle qu'en termes de microéconomie, l'économie « électronique » a, depuis 1995, fondamentalement changé la façon de conduire les affaires et qu'elle continuera de modifier le fonctionnement des marchés à l'avenir. Il présente des chiffres qui illustrent de manière éloquente la croissance du commerce en ligne.

M. Schlögl passe en revue les travaux de l'OCDE sur la politique en matière de commerce électronique et mentionne la Conférence ministérielle d'Ottawa de 1998 et le programme de travail en cours de l'OCDE dans les domaines de la protection de la vie privée et du consommateur. Il souligne que renforcer la confiance est un enjeu important de la nouvelle économie et de la société mondiale de l'information. Il remarque notamment que l'élément clé du renforcement de la confiance consiste à garantir aux usagers et aux consommateurs des voies de recours efficaces en cas de litiges nés d'échanges et de transactions en ligne. Toutefois, pour que le RAL en ligne développe son plein potentiel, surtout dans le cadre de règlement de litiges transfrontières entre entreprises et consommateurs, des questions juridiques complexes et des questions techniques tout aussi complexes doivent être abordées : à cette fin, il encourage les participants à la conférence à exploiter leurs divers domaines d'expertise pour trouver des solutions pratiques dans ce domaine.

Mme Maria Livanos Cattaui, Secrétaire générale de la Chambre de Commerce internationale, présente le pointe de vue des milieux d'affaires mondiaux et de la CCI qui, depuis 80 ans, fait figure de pionnière en matière de règlement des différends commerciaux. Elle déclare que toutes les parties prenantes ont un rôle différent à jouer dans la mise en place de RAL efficaces dans le monde, et que bâtir des partenariats entre des parties prenantes disposées à y consacrer du temps et des efforts est un pas fondamental dans cette direction.

Mme Cattaui explique quel doit être le rôle respectif des diverses parties prenantes. Elle déclare que les autorités publiques peuvent apporter leur poids politique et créer une instance commune mais qu'ils doivent s'abstenir de restreindre les avantages des RAL. Les systèmes d'accréditation ou d'agrément ne doivent en aucun cas être obligatoires, ils doivent tenir compte des principes et des règles internationales d'auto-réglementation, en respectant la transparence et l'ouverture là où ils s'appliquent. Les autorités publiques doivent promouvoir activement les systèmes de RAL en tant que solution alternative aux règlements judiciaires. Ils ne doivent pas laisser se former des obstacles à l'innovation, particulièrement dans le domaine de la confidentialité et de la sécurité sur l'Internet. Enfin, ils doivent être aussi ouverts aux efforts de tous les acteurs.

Mme Cattaui estime que les représentants des milieux d'affaires mondiaux pourraient fournir des ressources pour promouvoir le RAL mais que leurs approches doivent continuer de s'adapter aux besoins des consommateurs et aux responsabilités des autorités publiques. Cela suppose de veiller à ce que les réclamations de clients soient traitées par les entreprises elles-mêmes avant d'être soumises à un mécanisme de RAL. Cela signifie également que les entreprises doivent être prêtes à coopérer avec des consommateurs où qu'ils se trouvent dans le monde et quelles que soient leur culture et leur langue.

Les organisations de la société civile, et notamment les associations de consommateurs, doivent être attentives aux besoins de ceux qu'elles représentent et doivent les convaincre que le RAL est fait

pour leur venir en aide, et que ces mécanismes sont économiques et justes. Elles doivent admettre que le rôle des autorités est de veiller à ce que le RAL offre à terme une solution optimale pour les deux parties. Les prestataires de RAL qui existent actuellement font œuvre de pionniers, et ils doivent donc rester souples pour s'adapter aux choix des consommateurs, gérant les procédures et les décisions de manière à garantir constamment l'impartialité, l'accessibilité, la transparence et la commodité du processus. Il est aussi de leur devoir de combler les fossés culturels et linguistiques. C'est sur les prestataires de RAL que pèse au bout du compte l'obligation d'efficacité, car c'est à eux qu'entreprises et consommateurs confient la résolution de leurs litiges.

Enfin, Mme Cattaui insiste sur le fait que toutes les parties prenantes, entreprises, autorités publiques, organisations de citoyens et prestataires de RAL, ne doivent pas avoir peur d'aller au fond des choses lorsqu'ils abordent les aspects sensibles du RAL, car ce serait contre-productif.

M. Hans van Loon, Secrétaire général de la Conférence de La Haye de droit privé international (CODIP), souligne l'importance de la coopération entre les parties intéressées dans le cadre d'un sujet tel que le RAL en ligne, qui est international et concerne les pays industrialisés comme les pays en développement.

M. van Loon établit une distinction entre l'environnement technologique et économique, véritablement mondial, et l'environnement juridique, mosaïque de systèmes nationaux, voire régionaux. Il souligne que, dans ce contexte, l'enjeu consiste à créer des liens entre des systèmes très divers. Il déclare qu'il est nécessaire d'établir un système ordonné pour accéder aux tribunaux nationaux et permettre aux tribunaux de rendre des décisions, et décrit les travaux de la Conférence de la Haye en ce sens. De plus, il est, selon lui, tout aussi important de promouvoir le RAL et d'établir à l'intention des citoyens des règles précises énonçant la procédure exacte à suivre si un accord ne peut être obtenu. M. Van Loon observe que le RAL international, combiné à des règles relatives au droit pertinent et à des politiques uniformes, a un avenir, mais que l'enjeu primordial est de trouver une formule permettant la coexistence du RAL et des décisions arbitrales.

Session 1 : État des lieux – Panorama des récentes discussions à propos du règlement alternatif des litiges en ligne

Thème : Afin d'offrir un forum, au niveau mondial, pour l'étude des modes alternatifs de règlement des litiges en ligne et d'encourager la coopération entre les acteurs, cette session avait pour but de faire le point des travaux entrepris sur ce thème par d'autres organisations. Elle devait mettre en lumière les similitudes et les différences qui existent entre les différentes approches connues à ce jour afin d'identifier les défis à relever et les lacunes à combler pour un règlement alternatif juste et efficace des litiges en ligne.

M. Risaburo Nezu, Directeur, Direction de la science, de la technologie et de l'industrie de l'OCDE, ouvre la session en soulignant qu'il est important de s'accorder sur des objectifs communs et sur les principes des modes de règlement alternatif des litiges et de bien prendre conscience des questions à étudier plus profondément.

Mme Carina Törnblom, Chef de section, Direction générale de la santé et de la protection des consommateurs de la Commission européenne (CE), fait le point sur les travaux de l'Union européenne en vue de trouver un moyen efficace de règlement des litiges entre entreprises et consommateurs. Elle explique que la CE, en coopération avec les entreprises et les consommateurs, s'est d'abord attachée à prévenir les problèmes pour les consommateurs et à encourager l'utilisation des meilleures pratiques commerciales. La CE a aussi étudié des voies de recours autres que les tribunaux, des codes de conduite dans le cadre de programmes de labellisation et des mécanismes de remboursement par carte de paiement.

Mme Törnblom souligne que la multiplication rapide de codes de conduite risque de permettre aux entreprises d'affirmer qu'elles adhèrent à un code de conduite sans pour autant résoudre le problème de la qualité du code et de son respect. A cet effet, elle déclare que les États membres de l'Union européenne doivent établir une base et des critères communs d'approbation des codes de conduite ; elle cite l'exemple de la Recommandation de 1998 applicable aux organes responsables pour la résolution extrajudiciaire des litiges publiée par la CE. Elle précise que la Recommandation s'est avérée utile et que les États membres ont déjà notifié la Commission des organes qui remplissent les critères que la Recommandation prescrit.

Mme Törnblom évoque également le réseau extrajudiciaire européen, un système de points centraux chargés de traiter les réclamations des consommateurs, dont la mise en place à l'échelle européenne est prévue avant l'été 2001. S'agissant des autres travaux portant sur le RAL, elle explique que l'UE envisage d'ajouter des règles aux réglementations qui régissent l'intervention des médiateurs et des conciliateurs. Enfin, Mme Törnblom souligne qu'il est important de permettre aux consommateurs d'avoir accès à leur propre système juridique tout en offrant un accès volontaire au RAL pour rendre inutile le recours aux tribunaux.

M. James Dorskind, Avocat conseil au Ministère du Commerce des États-Unis, communique certaines conclusions d'un atelier sur le règlement alternatif des litiges relatifs aux transactions des consommateurs sur un marché en ligne organisé en juin 2000 par le Ministère du Commerce et la Federal Trade Commission des États-Unis. Il souligne que les procédures qui fonctionnent entre entreprises ne conviennent pas nécessairement aux transactions entre entreprises et consommateurs. Pour que le RAL fonctionne dans le contexte entre entreprises et consommateurs, il doit être pratique pour les consommateurs et capable de protéger les informations les concernant. Il mentionne d'autres moyens de résoudre les litiges, les remboursements par carte de paiement par exemple. M. Dorskind explique que des entreprises de nature différente peuvent aborder le RAL de manière différente. Ainsi, les petites entreprises auront peut-être davantage besoin d'un prestataire tiers que des entreprises plus importantes. Il est par ailleurs probable que la meilleure méthode de règlement des différends varie selon la valeur de la transaction ou la complexité du litige. Il décrit quelques principes généraux sur le RAL, issus des débats qui ont eu lieu lors de l'atelier organisé aux États-Unis, ajoutant qu'il est prématuré d'en affiner la définition. Il s'agit des principes d'impartialité, d'accessibilité, de coût modique ou nul pour le consommateur (par rapport au montant sur lequel porte le litige), de transparence (les consommateurs devraient disposer des informations concernant le mécanisme avant de devoir décider s'ils acceptent une procédure de règlement alternatif des litiges), d'opportunité et de rapidité. Il précise qu'il n'y a guère de consensus entre les acteurs quant à savoir si le règlement alternatif des litiges doit être obligatoire ou pas.

M. Dorskind indique que le renforcement de la confiance des consommateurs passe par l'établissement de RAL mondiaux et transparents. C'est pourquoi le Ministère du Commerce travaille en collaboration avec l'UE pour encourager le secteur privé à élaborer des RAL adaptés à l'évolution du marché. Il insiste sur le fait que tous les acteurs devraient participer à ces discussions pour que des mécanismes justes et efficaces soient mis en place. M. Dorskind explique par ailleurs que les problèmes du droit applicable doivent être traités au niveau international, le règlement alternatif des litiges devant fonctionner convenablement dans différentes cultures nationales et juridiques.

M. Yuko Yasunaga, Directeur adjoint, Division de la politique du commerce du Ministère du commerce international et de l'industrie du Japon, présente les activités de l'APEC dans le domaine de la protection des consommateurs et du règlement alternatif des litiges. Il décrit la mise en place du Groupe directeur sur le commerce électronique (ECSG) et le Plan directeur de 1998 de l'APEC, qui confie aux entreprises un rôle de premier plan dans le développement du commerce électronique et charge les autorités d'assurer un environnement favorable à la croissance de ce commerce. Il évoque

l'atelier sur la protection des consommateurs organisé par l'ECSG à Bangkok en juillet 2000. Celui-ci a montré qu'il était nécessaire d'intensifier la coopération et la collaboration entre les acteurs de la région afin de niveler les différences qui existent entre les pays de l'APEC en termes de lois, de règles, de disponibilité de l'information et de sensibilisation en matière de commerce électronique. Les participants à l'atelier ont accepté d'échanger des informations sur les lois et réglementations portant sur la protection du consommateur et de chercher à développer leur coopération en ce qui concerne l'application de la loi.

M. Yasunaga présente plusieurs « modèles de meilleures pratiques » visant à renforcer la confiance des consommateurs en ligne mis en place par les pays de l'APEC, notamment les projets de codes de conduite de l'Australie, le programme de labellisation pour les achats en ligne du Japon et le programme CaseTrust de Singapour, un programme de consultation dans le cadre de litiges piloté par le gouvernement. Il cite un exemple de coopération en Asie, les pourparlers entre le Japon et la Corée portant sur l'agrément et la reconnaissance mutuelle des labels de confiance, et décrit l'atelier sur la protection des consommateurs organisé par l'APEC et l'ECSG à Bangkok en juillet 2000. M. Yasunaga souligne que le règlement alternatif des litiges en ligne est encore en phase initiale à l'APEC et qu'il revient essentiellement au secteur privé d'encourager l'utilisation de ces mécanismes. Il ajoute toutefois que les autorités publiques ont également un rôle à jouer, par exemple en favorisant l'utilisation des points centraux et d'autres moyens appropriés pour développer le recours au RAL et la diffusion d'informations pertinentes à son sujet.

Mme Constanze Picking, Directeur principal, Échanges et commerce en ligne, de Daimler Chrysler AG, expose les vues du Global Business Dialogue on e-Commerce (GBDe) sur le commerce électronique. Elle brosse les grandes lignes des travaux du GBDe sur le règlement alternatif des litiges en 2000, notamment ceux de chaque groupe de travail régional (Europe/Afrique, Amériques et Asie/Océanie) en vue d'inventorier les modes de règlement alternatif des litiges en ligne dans leur région, ainsi que de nombreux ateliers et réunions avec les parties prenantes.

Mme Picking décrit le document du GBDe sur les programmes de règlement alternatif des litiges en ligne rédigé pour la conférence annuelle de cet organisme en septembre 2000. Ce document contient des recommandations aux cybermarchands, aux prestataires de RAL et aux autorités publiques quant aux meilleurs moyens de développer le règlement alternatif des litiges en ligne. Le GBDe recommande aux cybermarchands d'encourager l'utilisation de programmes internes de satisfaction du consommateur et d'informer les consommateurs de l'existence et des conditions d'utilisation du RAL. S'agissant des prestataires de services, le GBDe spécifie que les modes de règlement alternatif des litiges devraient être impartiaux, accessibles, pratiques, rapides, peu onéreux pour le consommateur, transparents, qu'ils devraient autoriser une procédure contradictoire et que ses exécutants devraient être suffisamment qualifiés. En outre, les modes de règlement alternatif des litiges devraient permettre aux parties d'être représentées et spécifier les règles applicables à la procédure. Les prestataires de RAL devraient également sensibiliser les consommateurs au règlement alternatif des litiges en ligne. Enfin, le GBDe recommande aux autorités publiques d'arrêter définitivement les règles internationales relatives à l'instance compétente et au droit applicable, d'encourager l'utilisation de programmes de satisfaction des consommateurs, de ne pas établir de discrimination entre les différents modes de règlement alternatif des litiges, de ne pas instituer de critères obligatoires ou de systèmes d'agrément des RAL et de permettre, dans certains cas, le recours à des arbitrages contraignants dans le cadre de litiges entre entreprises et consommateurs.

Mme Picking évoque plusieurs questions non réglées, dont débattent encore les membres du GBDe, par exemple l'agrément de systèmes RAL et l'accréditation d'organismes de certification. Les prochaines mesures du GBDe dans ce domaine seront de créer un site Web destiné à développer la

confiance des consommateurs, de mettre en place des points centraux de règlement alternatif des litiges et d'engager des discussions avec des représentants des consommateurs.

Mme Louise Sylvan, Présidente de Consumers International, observe que les principes de Consumers International en matière de règlement alternatif des litiges en ligne et ceux présentés par le GBDe, l'UE et le DTAC se rejoignent et concordent sur de nombreux points. Elle présente un résumé de l'étude sur les prestataires de services de règlement alternatif des litiges en ligne réalisée par Consumers International et publiée le 11 décembre 2000. L'étude a évalué 30 programmes de règlement alternatif des litiges en ligne en fonction de huit critères : indépendance/impartialité, transparence, disponibilité, accessibilité pécuniaire, efficacité, équité (procédure de recours), légalité/liberté et surveillance par un tiers. Elle a conclu qu'aucun d'eux ne satisfaisait à l'ensemble des critères, quoique la plupart soient aisément accessibles, disponibles en temps utile, faciles à utiliser et qu'ils expliquent adéquatement la procédure. Mme Sylvan a cité plusieurs lacunes de ces mécanismes : nombre d'entre eux avaient une capacité limitée à régler les litiges dans plusieurs langues, la plupart étaient excessivement onéreux et peu rendaient compte de l'issue de la procédure de manière transparente. Elle indique que l'étude met en évidence des problèmes d'application des décisions issues de procédures de RAL et que la multiplication des programmes, qui déconcertera les consommateurs, porte préjudice au règlement alternatif des litiges. De plus, les intérêts des consommateurs sont moins représentés dans les structures régissant les programmes que ceux des entreprises.

Mme Sylvan propose, sur la base de l'étude, plusieurs recommandations pour les programmes de règlement alternatif des litiges en ligne. Les mécanismes doivent aussi s'adresser aux personnes non anglophones et doivent rendre compte des décisions de manière plus transparente. Par ailleurs, les coûts du RAL pour les consommateurs ne peuvent être supérieurs à ceux de la plupart des litiges entre entreprises et consommateurs, et les clauses inappropriées en matière de RAL obligatoire et d'arbitrage contraignant doivent être supprimées. Elle conclut que le règlement alternatif des litiges en ligne doit être assujetti à des normes mondiales et à une supervision permanente indépendante.

M. Nezu résume le débat en disant que s'il est clair qu'il n'existe pas de solution unique en ce qui concerne les programmes de règlement alternatif des litiges, la discussion a permis de cerner quelques éléments communs aux RAL et des moyens de mettre en place ces mécanismes. Il est notamment nécessaire d'assurer :

- Une coopération assidue de tous les acteurs.
- La transparence (c'est-à-dire fournir les informations essentielles dont les consommateurs ont besoin pour choisir un mode de règlement alternatif des litiges en connaissance de cause).
- Une accessibilité de haute qualité pour permettre aux consommateurs de faire appel aux systèmes de règlement alternatif des litiges à un coût modique tout en ménageant un équilibre entre le coût du RAL et le profit pour le consommateur.
- L'aplanissement des différences culturelles et linguistiques dans la procédure de RAL.
- Une prise de décision rapide.
- Un intermédiaire impartial et qualifié pour diriger le règlement alternatif des litiges.

M. Nezu ajoute qu'aucun des modes de règlement alternatif des litiges en ligne (dont la plupart sont très récents) ne satisfait à l'ensemble des critères ci-dessus et qu'ils doivent donc être améliorés. S'agissant des travaux ultérieurs dans ce domaine, il souligne que plusieurs personnes estiment qu'un

point central d'échange d'informations serait efficace. Il signale également deux questions non résolues qui méritent plus ample discussion : *i)* celle de savoir si le recours au règlement alternatif des litiges devrait être volontaire ou s'il pourrait être obligatoire, et si la décision issue de la procédure devrait être non contraignante ou contraignante ; *ii)* la nécessité de définir précisément le RAL et d'établir la distinction entre la procédure de règlement alternatif des litiges et celle des tribunaux.

Session 2 : Illustration des réclamations possibles entre entreprises et consommateurs dans l'environnement en ligne

Thème : Cette session avait pour objet de présenter des informations et des statistiques sur la nature et le volume des réclamations faites par les usagers et les consommateurs en relation avec leurs opérations et transactions en ligne afin de sensibiliser tous les acteurs sur les aspects qui doivent constituer les grands axes de l'étude des mécanismes de réparation et des modes alternatifs de règlement alternatif des litiges en ligne.

Mme Michelle Childs, Chef de la recherche en stratégie, Association des consommateurs (*Consumers Association)* (Royaume-Uni), présente les grandes lignes du programme de labellisation Web Trader, un partenariat européen regroupant des organisations de consommateurs de sept pays. A ce jour, 1 500 sociétés membres ont le label. Il s'agit d'un programme d'adhésion à un code de pratiques qui exige des cybermarchands, par exemple, qu'ils indiquent clairement les prix, tous frais compris, au consommateur, qu'ils effectuent les remboursements dans un délai maximum de 30 jours, qu'ils assurent la sécurité de leur site et disposent d'une procédure de gestion des réclamations. Des conditions d'admission rigoureuses leur sont appliquées, et le respect du code est surveillé en permanence.

Le programme Which?Web Trader recueille également les réclamations des consommateurs. En novembre 2000, les réclamations portaient essentiellement sur deux points : le non-respect des délais de livraison (226 réclamations sur plus de 740) et la mauvaise gestion des réclamations (107 réclamations sur plus de 740). En cas de litige, le code exige que le consommateur contacte d'abord le cybermarchand. Si celui-ci ne réagit pas comme il convient dans un délai de cinq jours, Which?Web Trader intervient. Les décisions de Which?Web Trader sont contraignantes pour le cybermarchand. Actuellement, Which?Web Trader n'assure pas de services de règlement des litiges internationaux et cherche à obtenir un financement de l'UE pour élargir ce service.

M. Stephen Lau, Commissaire pour la protection de la vie privée et des données personnelles, Région administrative spéciale de Hong Kong, Chine, présente les principaux éléments qui menacent la confidentialité des données sur Internet au regard de l'ordonnance sur les données personnelles de Hong Kong, Chine. Cette ordonnance établit six principes de protection des données, à savoir la finalité et le mode de collecte des données personnelles, l'exactitude et la durée de conservation des informations, l'utilisation des données personnelles, leur sécurité, les informations sur les données détenues et leur finalité, et l'accès des individus à leurs données personnelles. Les principales réclamations reçues par ses services concernent la collecte de données sans le consentement de l'intéressé, l'usurpation d'identité, l'interception de données au cours de transmissions et l'utilisation de données à des fins autres que celles qui ont initialement motivé leur collecte.

M. Lau résume ensuite les conclusions d'une vaste enquête conduite entre juillet et octobre 1998 sur 531 sites Web de Hong Kong, Chine, pour évaluer dans quelle mesure l'Ordonnance et les normes de gestion adéquate et raisonnable des informations personnelles étaient respectées. L'étude a conclu qu'en 1998, 6.2 % seulement des sites présentant des formulaires de collecte de données personnelles en ligne affichaient une déclaration de confidentialité. Ce chiffre est passé à 25 % en 1999. Seize sites qui présentent des formulaires à remplir mais n'offrent pas de déclaration de confidentialité font

actuellement l'objet d'une enquête officielle. Les services du Commissaire pour la protection de la vie privée ont depuis lors publié des lignes directrices sur la protection de la vie privée et les déclarations de confidentialité à l'intention des usagers individuels d'Internet et des exploitants de données pour les sensibiliser aux bonnes pratiques relatives à la vie privée dans le cyberespace et limiter ainsi les risques de violation de la vie privée.

Mme Maneesha Mithal, avocate au Bureau de la protection des consommateurs de la Federal Trade Commission (FTC) des États-Unis, donne une présentation générale de la base de données Consumer Sentinel, un projet commun de la FTC et du Ministère de l'Industrie du Canada. Les réclamations des consommateurs, émanant de sources publiques et privées, sont entrées dans la base de données et les fonctionnaires usagers peuvent examiner des réclamations spécifiques ainsi que les grandes tendances. Les réclamations concernant l'Internet ont connu une augmentation spectaculaire au cours des trois dernières années. Elles ont plus que doublé chaque année, passant de 872 en 1997 à 7 955 en 1998 et à 18 622 en 1999. Dans le même temps, la part de réclamations liées à l'Internet dans la base de données a aussi régulièrement augmenté, passant de juste 3 % en 1997 à 11 % en 1998 et à 22 % en 1999. Au cours de la dernière année, 10 % des réclamations concernaient des consommateurs américains et des sociétés étrangères tandis que 2 % concernaient des consommateurs étrangers et des sociétés américaines. Au cours des trois années écoulées, la FTC a constaté une hausse du nombre de réclamations liées à l'Internet qui concernaient des inexécutions de garantie et des violations de la règle de vente par correspondance. Mme Mithal recense également quelques-unes des réclamations relatives à la vie privée les plus fréquentes : courriers électroniques commerciaux non sollicités, usurpation d'identité, harcèlement téléphonique, fourniture d'informations sur la solvabilité sans le consentement de l'intéressé, vente de données à des tiers et protection de la vie privée des enfants. Enfin, elle précise que le règlement alternatif des litiges en ligne peut ne pas convenir aux réclamations contenant un élément frauduleux.

Mme Marcie Girouard, Assistante adjointe du Commissaire d'Industrie Canada, décrit le nombre et la nature des réclamations portant sur le commerce électronique déposées par les consommateurs auprès du gouvernement canadien, en précisant que les tendances en termes de consommation au Canada accusent un retard de deux ans par rapport aux États-Unis. Au cours des trois premiers trimestres de 2000, les réclamations concernant des opérations sur Internet ont représenté 2.2 % de l'ensemble des réclamations déposées auprès d'Industrie Canada. Parmi elles, 17.4 % portaient sur des transactions commerciales électroniques. Les plus fréquentes avaient trait à la non livraison de produits, aux délais de livraison, à la non communication des coûts et frais, aux caractéristiques des produits, et aux prix de vente au détail par rapport aux prix en ligne. Un nombre croissant de réclamations étaient déposées contre des sites établis en dehors du Canada.

Mme Girouard décrit également l'examen de 292 sites Web récemment conduit par Industrie Canada en fonction de critères choisis exposés dans les Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique de 1999. D'après les conclusions de cette étude, 77 % des cybermarchands communiquent le prix total de l'achat et 52 % expliquent leur politique d'échange et de retour des marchandises ; 26 % offrent des procédures de réclamation aux consommateurs et 16% seulement décrivent les mécanismes de règlement des litiges. Elle indique que la base de données sur les réclamations d'Industrie Canada et l'examen des sites Web permettent de conclure que les questions de protection du consommateur sont multijuridictionnelles, que les réclamations des consommateurs usagers de l'Internet couvrent un large éventail et que les modes de règlement alternatif des litiges ne sont pas encore disponibles partout.

Session 3 : Règlement des litiges au stade le plus précoce – Traitement interne des réclamations en ligne et remboursement des consommateurs

Thème : Cette session avait pour objet d'examiner le champ d'application et l'efficacité des systèmes internes de traitement des réclamations et de remboursement des consommateurs (suite à la mise en place de systèmes de remboursement par carte de paiement) pour régler les réclamations et les litiges entre entreprises et consommateurs.

M. Hugh Stevenson, Directeur associé, Bureau de la protection des consommateurs de la Federal Trade Commission des États-Unis, remplit les fonctions de modérateur pour cette 3e session.

M. Charles Underhill, Directeur opérationnel par intérim de l'Union des Better Business Bureau, décrit les grands axes du traitement des réclamations des consommateurs du BBB et présente quelques remarques sur le traitement interne des réclamations. Le programme AutoLine du BBB, qui traite les litiges concernant les automobiles, a reçu près de 33 000 réclamations en 1999. Un nombre considérable d'entre elles ont été réglées par le commerçant avant que le consommateur ne dépose officiellement plainte. Le BBB a traité la plupart des autres affaires par voie de médiation. En 1999 également, les bureaux locaux du BBB aux États-Unis et au Canada ont reçu des consommateurs plus de 3 millions de demandes d'assistance dans le cadre de réclamations. Le BBB a réglé 66 % de ces affaires.

M. Underhill décrit une enquête récemment menée par e-Satisfy sur le service à la clientèle des sites de commerce électronique. L'étude montre que les clients en ligne attendent des sociétés un meilleur temps de réponse que les clients ordinaires. Sur les deux tiers de contacts en ligne non satisfaits, un traitement inadéquat entraîne une baisse d'au moins 30 % du taux de fidélisation de la clientèle. Il signale que BBBOnLine encourage les cybermarchands à appliquer de meilleures pratiques commerciales par l'intermédiaire de son nouveau Code de pratiques commerciales électroniques, approuvé en mai 2000. Par ailleurs, le BBB a conclu une alliance avec Visa USA pour informer les cybermarchands américains de l'existence du Code et les sensibiliser aux questions de sécurité et de protection des données ; il vient également de former un partenariat avec PriceWaterhouseCoopers pour mettre au point un système de règlement en ligne des problèmes entre entreprises et consommateurs.

M. Alastair Tempest, Directeur général de la Fédération du marketing direct européen (FEDMA), évoque la nécessité de développer la confiance entre entreprises et consommateurs sur le marché en ligne. Il note que le programme « circuit de confiance » propose à cette fin un code de conduite, un mécanisme connexe de résolution des réclamations des consommateurs et des liens avec les systèmes de RAL en ligne. Il signale en outre que, selon la FEDMA, divers systèmes de médiation devraient être disponibles et que l'accent devrait être mis sur le multilinguisme. Mais, ajoute M. Tempest, le consommateur ne devrait jamais avoir l'impression qu'il est obligé de recourir à un mécanisme de règlement des réclamations ou à un mode de règlement alternatif des litiges. Le recours à une action judiciaire ne doit pas lui être refusé.

Mme Helen Bridges de American Express Services, Europe, analyse l'utilisation du mécanisme de remboursement par carte de paiement comme moyen de consolider la confiance des consommateurs.

Débat

Les réflexions suivantes sont issues de la discussion avec les panélistes et le public :

- Les règles relatives aux mécanismes de paiement ne s'appliquent pas de la même manière à toutes les cartes de paiement ; ainsi les règles, quand elles existent, sont différentes pour les cartes de débit et de crédit (Mme Jean Ann Fox, Directeur de la protection des consommateurs, Fédération des Consommateurs d'Amérique).
- Dans des pays comme la France, où il est impossible qu'un programme prévoie les remboursements par carte de paiement en raison de l'irrévocabilité des paiements du principal, on peut trouver un moyen d'assurer aux consommateurs les mêmes droits qu'aux États-Unis par exemple. A titre d'exemple, Visa demande que le détenteur de la carte tente d'abord de résoudre le problème directement avec le commerçant ; si le problème n'est pas réglé, le consommateur peut alors demander l'assistance de l'organisme émetteur de la carte (M. Peter Møller Jensen, Responsable des relations avec l'Union européenne à Visa International).
- On ne dispose pas de chiffres en ce qui concerne les remboursements. Toutefois, l'un des avantages pour les consommateurs est que les organismes émetteurs de cartes ont un vaste pouvoir de négociation et peuvent l'exploiter pour imposer des normes de meilleures pratiques aux commerçants. (M. Eric Mickwitz, Médiateur finlandais pour les consommateurs)
- Il n'est pas utile de considérer les remboursements comme des RAL. Ils sont un système de traitement des réclamations parmi d'autres, même s'ils vont plus loin que les systèmes habituels. Ils ne constituent pas un mode de règlement alternatif des litiges et ne satisfont absolument pas aux critères d'indépendance, de transparence etc. énoncés pour les RAL. (Mme Fox et M. Mickwitz).
- Il convient de noter qu'il faut encourager avec prudence les consommateurs à utiliser leurs cartes de crédit en ligne car le fait qu'un cybermarchand puisse accepter une carte de crédit ne témoigne en aucun cas de sa crédibilité.

Session 4 : Modes alternatifs de règlement des litiges en ligne

Thème : Cette session avait pour objet d'examiner, à travers la présentation des modes alternatifs de règlement des litiges en ligne, déjà existants ou en cours de développement, la grande diversité des approches possibles pour régler les litiges qui surviennent en ligne. Afin d'attirer l'attention sur les éléments spécifiques, procéduraux et autres, de ces divers mécanismes, la session a été divisée en trois parties. Le premier débat a été consacré aux mécanismes entièrement automatisés dont les résultats sont obtenus sans intervention de l'homme. Le deuxième et le troisième débat devaient examiner les autres mécanismes, d'un formalisme variable sur le plan de la procédure et faisant plus ou moins intervenir un tiers neutre. Enfin, le quatrième débat, en explorant les systèmes en cours de développement, a porté sur les objectifs et la méthodologie nécessaire pour mettre en place un mécanisme alternatif de règlement des litiges en ligne.

M. Bernard Clements, Chef de l'unité des sciences de la vie, de l'information et de la communication à l'Institut de Prospective Technologique (IPTS) du Centre Commun de Recherche de l'UE, à Séville anime les débats de la 4e session. Il rappelle que les sessions précédentes ont montré que le règlement alternatif des litiges ne convient pas pour tous les types de litiges. Par exemple il n'est pas adapté en cas d'escroquerie, d'absence de coopération du vendeur ou dans les affaires de protection de la vie privée. M. Clements propose à l'assistance de réfléchir à la question de savoir s'il

existe des types de litiges qui seraient mieux résolus par certaines catégories de RAL, et s'il faudrait adapter les mécanismes de RAL en fonction des litiges relatifs à la vie privée et à la protection des consommateurs dans le cadre entreprises-consommateurs, étant donné que les litiges relatifs à ce segment sont nombreux, qu'ils portent sur de faibles montants et impliquent un préjudice limité. Il ajoute que cette session a pour objet de mettre en évidence les problèmes et les difficultés liées à l'application des différents types de mécanismes de RAL et donc d'aider les parties prenantes à définir les aspects essentiels d'un RAL juste et équitable entre entreprises et consommateurs au cours des sessions suivantes de la conférence.

Session 4-I : Mécanismes entièrement automatisés de règlement des litiges en ligne

Thème : la plupart des systèmes automatiques de règlement alternatif des litiges sont destinés à résoudre les litiges pécuniaires, notamment en matière d'assurance, et supposent que les parties conviennent, avant d'entrer en négociation, de se conformer à la solution si le litige se règle. L'objet de cette session est d'examiner si ces systèmes peuvent contribuer à régler les litiges entre entreprises et consommateurs dans le domaine de la protection des consommateurs et de la vie privée.

M. Richard Belczynski, Vice-président de la Division internationale et commerciale de ClickNSettle.com, décrit l'une des formes de règlement alternatif des litiges de son entreprise, la procédure d'offre aveugle en ligne qui permet de résoudre les litiges en matière d'assurance et d'ordre pécuniaire. M. Belczynski explique que ce système est prévu pour des parties qui ont déjà négocié et n'ont pas résolu leur litige. Chacune d'elles s'inscrit sur le site Web et est autorisée à entrer le montant du règlement souhaité. Si les offres des parties se situent dans une fourchette de 30 % l'une de l'autre, l'affaire se règle ; dans le cas contraire, les parties sont notifiées et peuvent présenter de nouvelles offres. Aucune partie ne peut consulter les offres de l'autre, mais peut voir si l'autre partie a soumis une offre et à quel moment. Avant d'entamer la procédure, les parties conviennent que le résultat sera juridiquement contraignant. Si aucun règlement n'intervient dans un délai de 60 jours, les parties peuvent recommencer la procédure ou opter pour un mode de règlement classique, un arbitrage hors ligne par exemple.

Débat

M. Ethan Katsh, Directeur du Centre pour les technologies de l'information et le règlement des litiges de l'Université du Massachussets, note qu'à ce stade liminaire du développement des mécanismes alternatifs de règlement des litiges en ligne, il existe de grandes différences entre les fonctionnalités techniques des systèmes. Certains sont beaucoup plus simples que d'autres, et sont moins onéreux, comme les systèmes automatisés « de type arbitrage ». Néanmoins, dans les cas de fraude présumée ou quand une intervention humaine est nécessaire, les systèmes entièrement automatisés ne peuvent offrir une solution appropriée.

M. John Borking, membre du Commissariat à la vie privée des Pays-Bas, se demande si la technologie permettrait au système d'agir comme un agent intelligent, c'est-à-dire d'apprendre la jurisprudence et de l'appliquer comme il convient pour aboutir à des décisions.

Il s'ensuit un débat sur la capacité de ces systèmes entièrement automatisés à régler les litiges types en matière de consommation.

- Il semble que le champ d'application du modèle de ClickNSettle soit limité à des réclamations de type dommages et intérêts et que l'utilisation d'un RAL de ce genre nécessite l'assistance d'un avocat (M. John Borking). M. Belczysnki confirme que le

système peut s'avérer limitatif quand des aspects plus humains entrent en jeu. Il précise également que 70 % des consommateurs qui y font appel ont des avocats et que 30 % l'utilisent par eux-mêmes.

- Le modèle ClickNSettle ne peut s'appliquer que de façon très limitée aux litiges types portant sur les achats ; il semble couvrir les règlements purement pécuniaires dans les cas où le consommateur est disposé à transiger (Mme Pippa Lawson, Avocate au Centre de défense des intérêts du public).

La question de la divulgation de l'issue des affaires est aussi débattue.

- ClickNSettle offre un système d'information qui permet aux clients de consulter les affaires les concernant. Du point de vue du consommateur, ce mécanisme crée un déséquilibre ; les compagnies d'assurance qui utilisent souvent le système peuvent consulter toutes les affaires dans lesquelles elles ont été impliquées, un consommateur n'ayant en revanche accès qu'à sa propre affaire. Pour instaurer un système symétrique d'information, on peut proposer de publier les informations accessibles au public sur les affaires (M. Underhill).

Enfin, Mme Dana Haviland, Associée de Wilson Sonsini Goodrich & Rosati, demande quelle est l'expérience de ClickNSettle à l'échelle internationale et suggère que pour garantir l'application des décisions à l'étranger, il faudrait peut-être mettre en place des mécanismes supplémentaires, des dépôts fiduciaires par exemple. M. Belczynski répond que le programme existe depuis 13 mois et, à ce stade, à surtout traité des affaires nationales. Dans le cas d'affaires internationales, aucune décision de la société n'a encore été contestée, mais elle envisage de recourir à des dépôts fiduciaires à l'avenir.

Session 4-II : Mécanismes de règlement souples

Online Resolution, Inc.

M. Colin Rule, Directeur général de Online Resolution, Inc., décrit dans les grandes lignes le système de règlement des litiges de onlineresolution.com en insistant tout particulièrement sur son outil de collaboration en ligne, Resolution Room. Online Resolution a accès à un réseau de 500 médiateurs et arbitres et règle toute une gamme de litiges concernant les consommateurs, les entreprises, les familles et le lieu de travail. Un outil de conseil en ligne aide les consommateurs à choisir le mode alternatif de règlement des litiges le mieux adapté à leur cas. Resolution Room est un environnement sécurisé sur le Web. Il regroupe des forums de discussion, des forums de consultation privés, un outil de vote et une fonction calendrier que le tiers neutre peut configurer pour l'adapter au mieux aux besoins des parties. Aucune information au sujet des litiges n'est envoyée par courrier électronique, puisque, d'après M. Rule, ce procédé, de par sa nature, n'offre aucune sécurité. Dans le cas de litiges portant sur des sommes inférieures à 500 USD, on facture 20 USD aux consommateurs ; pour les litiges portant sur une somme supérieure à 500 USD, chaque partie est facturée à l'heure du tiers neutre. L'accès à la Resolution Room est facturé en fonction d'un barème. Dans le cas de transactions portant sur de faibles montants, le site n'est utilisé que peu de temps et les frais sont relativement bas.

SquareTrade

Mme Cara Cherry Lisco, Directeur du réseau de règlement des litiges en ligne de SquareTrade, présente ensuite le modèle de Square Trade et insiste notamment sur le fait que la technologie peut constituer un outil efficace pour aider à résoudre les litiges portant sur de faibles montants, mais nombreux. Dans un premier temps, Square Trade permet aux parties de négocier directement entre elles pour tenter de régler leur différend. Si cette démarche échoue, le litige entre en phase de médiation. L'outil de négociation directe est gratuit pour les consommateurs. Mme Lisco explique que lorsque Square Trade a lancé ce système, 30 % des affaires seulement aboutissaient à un règlement mais, grâce aux progrès techniques, le taux de règlement des litiges atteint aujourd'hui 80 %. Un élément important du système est le formulaire de réclamation en ligne, qui n'est pas un outil statique mais plutôt un « guide intelligent » qui propose différentes options selon les réponses à la question précédente. Ce système aide les parties à mieux définir leurs problèmes et leurs exigences. Mme Lisco décrit un autre outil utile aux usagers, la présentation de données sur le règlement de litiges similaires. A la date de la conférence, la société a résolu plus de 30 000 affaires, dont 12 % à 15 % à l'échelle internationale.

Mme Lisco analyse quelques-uns des problèmes de confidentialité et de vie privée qui surgissent dans le cadre du règlement alternatif des litiges en ligne. Square Trade maintient une base de données de réclamations contre les entreprises détentrices d'un label : la question de savoir qui devrait avoir accès à ces informations et quelles informations pourraient être divulguées n'est pas encore réglée. Par ailleurs, Square Trade n'a pas encore déterminé s'il convient de publier les résultats des affaires ou pas.

Débat

Suivent des questions des panélistes quant à la capacité du consommateur lambda à utiliser les outils de Resolution Room et à la formation des tiers neutres. M. Rule répond que le système Resolution Room a été testé par des consommateurs de plusieurs pays et semble être très accessible et facile à comprendre. Le système fait appel à des fenêtres et à des animations instantanées et a fait l'objet de démonstrations dans de nombreux pays. Les tiers neutres sont des spécialistes dans leurs domaines. Chacun reçoit une formation de 60 heures pour apprendre à utiliser efficacement ses compétences en matière de médiation et d'arbitrage en ligne.

Des questions sont également posées à propos des types de litiges traités et du délai nécessaire à leur règlement. M. Rule explique que le programme a été élaboré pour résoudre les litiges qui surgissent en ligne mais que le marché de la société couvre aujourd'hui des affaires hors ligne. Il explique aussi que 90 % des affaires sont réglées en moins de deux heures de temps du tiers neutre au total.

Mme Odile Nicolas-Etienne de l'*Union Fédérale des Consommateurs*, souligne que les consommateurs doivent avoir les moyens de définir si le règlement alternatif des litiges est le moyen le mieux adapté à leur cas. Il leur faut pour cela disposer d'informations sur les RAL. Elle se dit déçue que les prestataires de services de règlement alternatif des litiges ne fournissent pas d'informations sur l'issue des procédures de règlement.

Mme Pippa Lawson appelle l'attention sur la structure de coûts élevés de la plupart des prestataires de services RAL en ligne qui apparaît dans le rapport de Consumers International. Elle remercie M. Rule d'avoir précisé que sa société cherche à mettre en place une nouvelle structure

tarifaire. Mme Lawson soulève également la question selon laquelle la médiation est la démarche la plus appropriée lorsque les deux parties doivent transiger. Elle insiste sur le fait que dans certaines situations, les consommateurs ne doivent pas être obligés d'accepter un compromis ; le règlement des litiges en ligne offre peut-être un moyen de réparation plus efficace, mais il ne s'agit pas pour autant d'éviter à tout prix le recours aux tribunaux.

M. Borking met en garde contre la divulgation des informations car elle découragerait les entreprises de recourir à la médiation. Mme Lawson remarque qu'entre les modèles de onlinedisputes.com et de Square Trade, celui de Square Trade semble mieux convenir au litige de consommation type puisque la plupart des différends, s'ils ne sont pas réglés par les mécanismes internes de traitement des réclamations, peuvent l'être au premier stade par négociation directe.

La question de la pertinence du règlement alternatif des litiges en ligne pour résoudre les litiges concernant la vie privée est débattue. Certains estiment que dans le cas de litiges simples, certains des systèmes présentés pendant cette session pourraient s'appliquer. M. Borking souligne que son gouvernement (celui des Pays-Bas), a reçu un financement de la CE pour développer un logiciel intelligent capable de traiter des affaires plus complexes, portant par exemple sur la vie privée des consommateurs.

Enfin, Mr. Borking soulève la question de l'outil-conseil qui aide les consommateurs à décider du type de RAL qui leur convient et demande si onlinedisputes.com affiche une dénégation de responsabilité. M. Rule répond que la société affiche effectivement une dénégation de responsabilité, indiquant aux consommateurs que l'outil-conseil n'est pas un conseil juridique et leur suggérant de s'assurer les services d'un avocat pendant la procédure de règlement.

Une question est posée par un membre de l'assistance au sujet de la surveillance de la qualité des prestations du tiers neutre et des disparités entre les parties en matière d'expression écrite. M. Rule souligne les avantages du règlement alternatif des litiges en ligne en précisant que toutes les informations échangées entre un tiers neutre et les parties sont saisies et peuvent donc être aisément soumises à un contrôle de qualité. Par ailleurs, la communication asynchrone peut s'avérer utile pour ceux qui ont des difficultés à s'exprimer par écrit parce qu'elle donne le temps aux parties de préparer leurs réponses au lieu de les forcer à donner une réponse verbale immédiate. Mme Lisco répond que le système de Square Trade comporte des déclencheurs automatiques qui, par exemple, les notifient si un médiateur n'a pas répondu à un client dans un délai de 24 heures ou si une affaire n'est pas réglée dans un délai d'une semaine, etc. Il existe d'autres mesures de contrôle de la qualité, comme l'examen des taux de satisfaction et de règlement des tiers neutres.

Session 4-III : Mécanismes de règlement formels

M. Fabien Gelinas Vice-président et Directeur juridique de eResolution, décrit les activités de sa société qui assure des arbitrages en vertu des règles relatives aux litiges concernant les noms de domaine de l'ICANN. Par ailleurs, eResolution vend également depuis peu des licences d'utilisation de sa technologie pour le règlement des litiges entre entreprises et des litiges dans le cadre de tout type de transaction commerciale. Dans le domaine du entreprises-consommateurs, eResolution fournira sa technologie au projet ECODIR, présenté dans la session 4-IV. Depuis sa création le 1er janvier 2000, eResolution a traité plus de 300 affaires faisant intervenir des parties venant de 45 pays. La société a récemment mis en place un système de gestion des documents pour le règlement alternatif des litiges en ligne. Cet outil, accessible sur l'Internet, permet aux parties et au tiers neutre de travailler sur un dossier depuis n'importe quel endroit. Il intègre une fonction de télécopie, un forum de discussion, et offrira bientôt une fonction de visioconférence. La société développe en outre un modèle de

médiation-arbitrage dans le cadre duquel le même tiers neutre peut jouer le rôle de médiateur et, le cas échéant, trancher les affaires. Selon M. Gelinas, les mécanismes d'application « souples » sont plus prometteurs que les méthodes fondées sur une approche légaliste.

M. Erik Wilbers présente dans les grandes lignes le système de règlement des litiges relatifs aux noms de domaine de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) et le développement de son programme de règlement alternatif des litiges en ligne. L'OMPI est en train d'établir une base de données électronique qui permettra aux parties d'accéder aux fichiers et à d'autres informations dans un environnement informatique sûr. Le système autorise les parties à soumettre des fichiers de toutes sortes, donne des notifications de soumissions, permet aux parties de régler leurs frais en ligne et offrira ultérieurement une fonction de visioconférence. M. Wilbers expose les règles relatives au règlement des litiges concernant les noms de domaines de l'ICANN et signale que l'année précédente, 1 682 affaires ont été présentées à l'OMPI, émanant de 74 pays. Plus de 1 100 d'entre elles ont été résolues, la durée moyenne de règlement étant inférieure à deux mois :880 des cas résolus l'ont été par le biais de décisions d'un groupe d'experts et 251 par des règlements entre parties.

Débat

Mme Haviland note qu'en ce qui concerne les RAL portant sur des litiges relatifs aux noms de domaines, il est primordial que les arbitres soient formés et très qualifiés puisqu'ils assument les fonctions de « juges » dans ce qui est *de facto* un tribunal commercial international. Bien que les règles de l'ICANN stipulent que les conclusions des affaires portant sur les noms de domaines soient rendues publiques, elle n'est pas convaincue que ceci doive s'appliquer aux litiges entre entreprises et consommateurs puisque, dans le cas des noms de domaine, l'objectif est d'établir un précédent, ce qui n'est pas le cas des transactions entre entreprises et consommateurs. D'autres suggèrent qu'il serait peut-être possible d'inclure des clauses de divulgation dans les conditions pré-litige régissant les transactions.

Un débat s'ensuit quant à la partialité potentielle de la procédure de l'ICANN. Les représentants des consommateurs affirment que les arbitres de l'OMPI se prononcent plus souvent en faveur des propriétaires d'une marque déposée de nom de domaine que des déposants, ce qui explique le nombre relativement important de litiges soumis à l'OMPI. Les prestataires de services de règlement alternatif des litiges argumentent qu'il s'agit d'une question de perception.

M. Ethan Katsh déclare que l'arbitrage dans l'environnement entreprises-consommateurs est difficile ; en effet, si quelques parties préfèrent l'arbitrage, il sera toujours difficile de persuader les autres d'y participer. Il recommande que le recours à l'arbitrage ne soit pas obligatoire ou qu'il soit régi par un accord d'arbitrage entre les parties. M. Katsh rappelle aux participants à la conférence que le règlement des litiges relatifs aux noms de domaines en est à ses balbutiements. Il indique qu'il existe trois grands organismes de règlement des litiges relatifs aux noms de domaines, dont l'un fait essentiellement appel à des spécialistes de l'IP, un autre à des universitaires et le dernier à des juges américains retraités. Il dit qu'il pourrait être intéressant d'étudier l'influence de ces différentes classes de tiers neutres sur les résultats des règlements.

Session 4-IV : Modes alternatifs de règlement des litiges en cours de développement

M. Duncan McDonald de l'*Institut américain d'études allemandes contemporaines* (AICGS) présente une proposition de l'AICGS en vue de créer un réseau commun d'entreprises allemandes et américaines pour régler les différends entre entreprises et consommateurs dans ces pays. L'objectif de

ce projet est de contourner les systèmes juridiques et de minimiser le rôle des juristes. Il est prévu que le système sera gratuit pour les consommateurs, non contradictoire, volontaire et non contraignant. Pour donner aux consommateurs la liberté de travailler avec un tiers neutre dans le pays où ils vivent ou ont acheté le produit, les services de tiers neutres seraient assurés par les universités. Les questions importantes à traiter concernent notamment la formation des tiers neutres à gérer ce type de travail, à traiter avec des consommateurs qui ne connaissent pas les règles de l'autre pays et à concevoir un système très simple adapté à la majorité des consommateurs qui ne veulent ni lire, ni écrire.

M. Vincent Tilman, chercheur au *Centre de Recherches Informatique et Droit*, décrit le projet ECODIR (Résolution électronique des disputes commerciales), actuellement en développement et financé par la CE, qui a pour objectif de mettre en place une procédure de règlement alternatif des litiges en ligne pour résoudre les litiges pan-européens, transfrontières, entre entreprises et consommateurs. Le projet, qui doit être lancé en juin 2001, tient compte des études portant sur les aspects sociaux, juridiques et techniques du règlement alternatif des litiges. Les parties prenantes au projet sont les universités européennes et nord-américaines, les centres de médiation, des sociétés du secteur privé, un conseil consultatif regroupant des représentants d'entreprises et d'organisations de consommateurs et des organismes extrajudiciaires nationaux. A ce jour, les organisateurs ont cerné plusieurs obstacles au respect des critères de règlement alternatif des litiges en ligne, notamment :

- Indépendance : comment financer le RAL dans le cas de litiges portant sur de faibles sommes ?
- Transparence : comment ménager un équilibre entre la quantité d'informations et la simplicité des informations à fournir aux consommateurs ?
- Le principe du contradictoire et comment protéger la confidentialité au cours de la procédure de médiation.
- Efficacité et légalité.

M. Christopher Kuner, Avocat chez Morrison & Foerster, LLC, présente les stratégies de la Chambre internationale de commerce dans le domaine du règlement alternatif des litiges entre entreprises et consommateurs. M. Kuner rappelle que la CCI possède le plus important forum d'arbitrage entre entreprises au monde et que, en tant qu'organisation commerciale de référence dans le monde, elle s'intéresse tout particulièrement au domaine entreprises-consommateurs. De plus, la CCI a une grande expérience de l'arbitrage et elle est bien placée assumer le rôle de chef d'orchestre dont la communauté mondiale des entreprises a besoin. Il précise qu'un groupe d'experts a été formé, selon des critères de diversité géographique et professionnelle, et a publié un document sur les questions stratégiques et les mesures concrètes à prendre. Les principes que met en évidence le document s'adressent aux entreprises, aux autorités publiques et aux prestataires de RAL, et ont pour but de satisfaire des impératifs tels que la disponibilité (le règlement alternatif des litiges doit être accessible lorsque l'on procède à des transactions), la crédibilité (notification des conditions régissant le règlement alternatif des litiges), la concurrence (offre de plusieurs modes alternatifs de règlement des litiges) et l'ouverture.

Parmi les mesures concrètes qu'il recense, le document mentionne l'établissement d'un point central de règlement des litiges qui aurait les fonctions suivantes :

- Fournir aux entreprises et aux consommateurs des informations relatives au règlement alternatif des litiges dans le monde.
- Assister les parties à la recherche d'un règlement alternatif des litiges.

- Fournir des formulaires standard en ligne pour la soumission d'affaires au RAL.
- Assurer des services de traduction.
- Élaborer des normes de base pour les prestataires de services de règlement alternatif des litiges.

Enfin, M. Kuner signale qu'il est envisagé d'offrir ultérieurement aux entreprises une assistance dans la fourniture de services internes aux consommateurs et dans la mise en place de leur propre système de règlement alternatif des litiges. A cette fin, il souligne que la CCI a l'intention de travailler en étroite coopération avec le GBDe et les groupes de consommateurs.

Débat

Les panélistes discutent deux questions qui présentent des difficultés pour l'établissement de modes alternatifs de règlement des litiges en ligne ; celle du recours obligatoire au règlement alternatif des litiges et celle de l'indépendance des systèmes de règlement alternatif des litiges.

- A ce stade liminaire du développement des modes alternatifs de règlement des litiges en ligne, la nature contraignante de l'arbitrage le rend moins attrayant pour les consommateurs. (M. Charles Underhill)
- Le caractère non obligatoire des modes alternatifs de règlement des litiges incite les prestataires à élaborer des systèmes efficaces, qui respectent les normes minimales et sont ainsi susceptibles de gagner la confiance des consommateurs. Les consommateurs ne devraient pas être assujettis à une obligation, contrairement aux entreprises. (Mme Pippa Lawson)
- Le RAL n'est qu'un outil destiné à développer la confiance des consommateurs qui, dans tous les cas, viendra essentiellement du respect par les entreprises de tous les aspects de la transaction. L'indépendance des systèmes de règlement alternatif des litiges devrait être assurée par l'utilisation de fonds collectifs auxquels contribueraient les entreprises de commerce électronique. (Mme Odile Nicholas-Etienne)

Deuxième jour : mise en place de modes alternatifs efficaces de règlement des litiges en ligne au niveau mondial

Mme Jytte Ølgaard ouvre la deuxième journée de la conférence en déclarant qu'il est important de discuter en quoi le règlement alternatif des litiges peut devenir un outil capable de développer la confiance des consommateurs sur le marché des transactions en ligne. Elle présente les thèmes, axés sur les questions juridiques et techniques relatives au RAL, qui seront abordés au cours de la journée. Se fondant sur les exposés de la journée précédente, elle donne son avis sur les conditions qui doivent régir le règlement alternatif des litiges en ligne, notamment l'impartialité, la facilité d'accès, la modicité du coût, la transparence et la fiabilité. Mme Ølgaard précise qu'il est également important de déterminer l'instance de supervision compétente de ces modes alternatifs de règlement des litiges.

Session 5 : Les défis au règlement des litiges en ligne

Session 5-I : Questions socio-économiques liées aux modes alternatifs de règlement en ligne

Thème : Cette session était axée sur l'étude de quelques-uns des défis socio-économiques, notamment l'impact des différences culturelles, linguistiques et économiques sur l'efficacité des RAL ou, de même, celui des différences d'information et d'expertise sur l'utilisation et la mise en œuvre des RAL, en tenant compte du fait que les moyens de communication en ligne (numérisation des textes, des sons, des images fixes ou vidéo) influencent les méthodes de travail, les schémas culturels et les styles de vie.

Mme Anna Fielder, Directeur du Bureau pour les économies développées et en transition de Consumers International, assure les fonctions de modérateur à la première séance de la 5e session. Elle soulève trois points, débattus au cours de la première journée, qui sont liés au thème de la présente session. Premièrement, l'idée d'asynchronisation des communications dans les modes alternatifs de règlement des litiges en ligne et les avantages qui peuvent dériver du fait que les parties ont le temps de réfléchir avant de répondre. Deuxièmement, la possibilité que les modes alternatifs de règlement des litiges en ligne contribuent à l'élimination de la partialité et des préjugés en matière de race, de sexe ou d'âge, par exemple. Enfin, elle souligne que les modes alternatifs de règlement des litiges en ligne risquent d'accentuer les déséquilibres en termes d'expression écrite ; ceux qui écrivent bien bénéficient d'un avantage en ligne.

Mme Nora Femenia, Professeur et Vice-présidente de OnlineDisputes.org, présente les conclusions de sa recherche approfondie sur les aspects sociaux du règlement alternatif des litiges et sur la manière dont les différences culturelles influencent l'utilisation et la mise en œuvre de modes alternatifs de règlement des litiges. Elle signale que des études ont montré que lorsque le médiateur est anglo-saxon, les parties non anglo-saxonnes perdent systématiquement. Elle explique que chaque culture a une notion différente du litige et que si l'on étudie les comportements culturels au cours d'une médiation, on peut établir une distinction fondamentale entre : *i)* les individualistes (axés sur le gain personnel) et *ii)* les collectivistes (axés sur le bien de la collectivité). Il est important d'observer le comportement des gens et de voir s'ils sont individualistes ou collectivistes, car ces deux types abordent un litige différemment, l'individualiste cherchant à obtenir réparation, le collectiviste cherchant à obtenir le meilleur résultat pour la collectivité et pour sa relation avec l'autre partie.

Elle souligne d'autre part qu'il est très important que les clients aient l'impression d'avoir reçu un traitement juste lors d'une procédure de règlement d'un litige. Elle rappelle ce qu'ont dit la veille d'autres orateurs ; les clients qui présentent une réclamation et dont la réclamation est traitée correctement reviennent, sont plus fidèles et dépensent plus qu'auparavant. Elle signale aussi qu'en général, les gens veulent de la sympathie, de la compréhension et être traités comme des clients importants.

Mme Femenia souligne par ailleurs que les clients attendent d'une procédure de règlement des litiges qu'elle comporte un traitement expert de la réclamation, des excuses de l'autre partie, et un mécanisme rapide et simple. Les clients accepteront une décision générée par un ordinateur (automatisée) parce que les ordinateurs sont perçus comme des parties neutres.

Elle précise que certaines cultures ne prédisposent pas à porter plainte. Les entreprises doivent donc fournir à ces clients une assistance qui tient compte de cette différence. Elle explique que certains désirs des clients transcendent toutefois les cultures : la présentation d'excuses ; la reconnaissance du client en tant que personne ; que l'entreprise ne nie ou n'excuse pas ses torts ; l'identification rapide du problème ; un traitement respectueux et attentif ; avoir la possibilité de laisser libre cours à ses émotions. Mme Femenia ajoute que les entreprises devraient offrir une réparation symbolique au consommateur pour le temps qu'il a consacré à la réclamation et que tout mécanisme de règlement

d'un litige devrait être gratuit et conçu du point de vue du consommateur. Enfin, elle insiste sur le fait que les clients ne devraient pas être inondés d'informations mais plutôt obtenir les informations nécessaires en temps voulu.

Débat

- La possibilité pour un consommateur de soumettre une réclamation dans sa langue maternelle est une composante intégrale d'un système accessible. L'expérience de l'Alliance européenne pour l'éthique en publicité (AEEP), qui compte 28 membres dans 25 pays et traite 50 000 réclamations (nationales et internationales) par an dans plusieurs langues, montre que pour un RAL réussi, il est essentiel avant toute chose de résoudre de manière adaptée le problème de l'obstacle linguistique. (Mme Carmen Fernandez Neira). Par ailleurs, quand on parle de langue, il ne s'agit pas simplement d'offrir une traduction littérale, mais de révéler le sens culturel implicite. Les sites de traduction en ligne devraient donc, outre traduire les textes, les adapter à la culture (Mme Femenia).
- La question des valeurs collectives par opposition aux valeurs individuelles dans le cadre d'un règlement de litige doit être prise en compte. Il existe plusieurs exemples de difficultés lors de médiations entre parties asiatiques, américaines ou européennes. La culture du médiateur peut aussi poser problème. Il est douteux que des systèmes automatisés de règlement des litiges puissent prendre en compte ces éléments humains complexes. (M Toh See Kiat, associé, Tan Peng Chin and Partners)
- Beaucoup de significations et d'interprétations différentes sont données au règlement alternatif des litiges. Même au sein de l'Union européenne, le peu d'informations à la disposition des consommateurs et les obstacles linguistiques sont une source importante de préoccupation (M. Giles Buckenham, Administrateur, Direction générale de la santé et de la protection des consommateurs de la Commission européenne)
- Il est important de développer un système qui tienne compte des différences culturelles. Les consommateurs veulent avoir l'impression que leurs réclamations sont traitées équitablement. Les parties prenantes ne devraient pas compter sur des modes alternatifs de règlement des litiges parfaits à ce stade : il est important de se montrer souple et de réfléchir aux moyens de créer et de mettre en œuvre des modes alternatifs de règlement des litiges mondiaux ou régionaux. (M. Scott Cooper, Directeur, politique des technologies de Hewlett-Packard)

M. Christopher Drahozal, Professeur à la Faculté de droit de l'Université du Kansas, donne une exposé portant sur les aspects économiques du règlement alternatif des litiges en ligne. En partant d'un principe de base de la science économique – selon lequel la rareté force les parties à faire des choix -, il a soulevé un certain nombre de questions à prendre en compte lorsque l'on examine le développement du règlement alternatif des litiges en ligne. Il souligne que certains litiges sont trop onéreux à résoudre, même en ligne. En revanche, le mécanisme en ligne étant susceptible de réduire le coût du RAL, il peut permettre de régler des différends qu'il serait peut-être trop onéreux de résoudre hors ligne. Il insiste néanmoins sur le fait qu'en l'absence d'un RAL en ligne à l'échelle mondiale, de nombreux litiges ne seront pas résolus, ou bien les décisions ne seront pas appliquées.

Il analyse la question de l'équité en ce qui concerne le coût du règlement alternatif des litiges et qui les assume ; tous les consommateurs n'ont pas de litiges. Or, les coûts du règlement alternatif des litiges seront répercutés sur le prix du produit et, en fin de compte, tous les consommateurs paieront le mécanisme de règlement.

M. Drahozal signale également que tous les litiges ne sont pas identiques. Des litiges de nature différente peuvent donc nécessiter des approches différentes. Par exemple, les litiges portant sur des achats de faible montant et ceux concernant des lésions corporelles sont complètement différents. Il observe que, d'un point de vue économique, il peut être efficace, dans certains cas, de supprimer le recours aux tribunaux par le biais d'une clause pré-litige d'arbitrage contraignant. Il reconnaît cependant qu'il est douteux que l'on renforce la confiance des consommateurs en leur demandant de se soumettre à un règlement alternatif des litiges obligatoire.

Débat

- Le premier obstacle à la confiance des consommateurs dans le commerce électronique est la méfiance envers l'outil lui-même. Le règlement alternatif des litiges n'offre pas une solution complète à ce problème. Il faut donner aux consommateurs plus d'assurances que, de toute manière, tout se passera bien. (M. Buckenham)
- De nombreux consommateurs hésitent à utiliser l'Internet. Le commerce électronique leur permet néanmoins d'économiser beaucoup de temps et d'argent, et ils peuvent obtenir de meilleurs services dans un environnement électronique. (M. Toh).

Mme Fielder clôt la session en notant qu'un consensus se dessine selon lequel le règlement alternatif des litiges doit être gratuit ou d'un coût modique pour les consommateurs et accessible. Pour rendre le règlement des litiges équitable et plus accessible, il faut résoudre les problèmes culturels et linguistiques.

Session 5-II : Questions juridiques liées aux RAL en ligne

Thème : Cette session devait mettre en lumière les aspects procéduraux et substantiels considérés comme essentiels pour garantir une procédure équitable et efficace, tout en reconnaissant qu'ils sont susceptibles de varier selon le type de RAL et/ou de litige.

M. Mozelle Thompson, Commissaire à la Federal Trade Commission des États-Unis, assure les fonctions de modérateur à la 2e séance de la session 5. Il soulève, au nom de M. Philippe Fouchard, professeur à l'Université de Paris II, quatre importantes questions juridiques à traiter : *i)* préserver le recours volontaire aux tribunaux ; *ii)* garantir la transparence du statut des intermédiaires ; *iii)* promouvoir des procédures souples ; *iv)* assurer la confidentialité, sauf accord contraire des parties.

M. Christopher Kuner présente la synthèse d'une étude sur les obstacles juridiques aux modes alternatifs de règlement des litiges en ligne qu'il a réalisée pour le compte du GBDe. Il reconnaît qu'il n'existe pas de consensus sur les différentes procédures et que des termes fondamentaux tels que « arbitrage » sont compris différemment, du fait des différences culturelles. Examinant les systèmes extrajudiciaires de règlement des litiges conduits par des tiers, M. Kuner explique que le RAL doit se fonder sur un accord entre les parties. Il ajoute qu'il n'est de l'intérêt de personne de contraindre une partie à un arbitrage contre son gré. Il analyse ensuite s'il convient d'envisager l'agrément des modes alternatifs de règlement des litiges. Il soulève d'autres problèmes juridiques relatifs aux RAL en ligne, par exemple la difficulté à déterminer le lieu de l'arbitrage en ligne ou le fait que les lois nationales sur le chiffrement pourraient compliquer les choses. Il évoque la sécurité en ligne et observe que les déficiences de l'Internet pourraient aller à l'encontre des garanties constitutionnelles de procédure équitable qui existent dans des pays comme l'Allemagne.

M. Kuner discute l'application des décisions dérivant des accords de règlement alternatif des litiges. Il ajoute qu'il est trop onéreux de procéder à l'application forcée des jugements sur la base de ces accords. Il analyse ensuite les décisions exécutoires. Il déclare ne pas croire que la Convention de New York soit utile dans le cadre du commerce électronique.

Débat

M. James Murray, Directeur du *Bureau Européen des Unions de Consommateurs (BEUC*), aborde la question des procédures obligatoires ou non obligatoires. Il préconise une procédure d'arbitrage non obligatoire, ajoutant que le RAL doit être une solution alternative à un procès mais qu'il ne faut pas imposer un choix rigoureux entre un procès et le RAL. Il souligne qu'il est très difficile de faire appliquer les règles juridiques. A cet égard, il recommande l'établissement de normes pour les modes alternatifs de règlement des litiges et propose que des tiers de confiance évaluent si une entreprise respecte ces normes ou pas. Il estime par ailleurs qu'il convient d'encourager une participation raisonnable des pouvoirs publics.

M. Ron Plesser, Associé de Piper Marbury Rudnick & Wolfe, évoque la possibilité d'un concept d'épuisement des recours. Il préconise un système qui exige des consommateurs qu'ils aient d'abord recours au RAL ; si, après cette démarche, le consommateur n'est toujours pas satisfait, il peut alors saisir les tribunaux. Cette méthode n'éteint pas les droits des consommateurs. Il argumente que les entreprises vont investir des sommes considérables dans la mise au point et l'entretien des systèmes de RAL, et qu'il est donc juste que les consommateurs soient obligés d'y recourir dans un premier temps. Il ajoute que, en ce qui concerne les normes, la question épineuse consiste à déterminer s'il convient d'accepter la législation d'une juridiction donnée. Il suggère qu'il serait peut-être plus facile de créer des codes pour différents types de procédures et d'étudier comment les appliquer.

Mme Petra Spring-Reiman, Direction générale du Marché intérieur de la Commission européenne, observe que, en ce qui concerne la question des RAL contraignants ou non contraignants, les juristes de droit romano-germanique conviennent probablement que l'éventualité de la mise en place d'un système quasi-judiciaire poserait problème. A cet égard, elle explique que si le RAL était contraignant, ses décisions constitueraient une sorte de précédent ; les juristes les étudieraient donc, dans un souci de cohérence, ce qui pourrait conduire à l'établissement de nouveaux principes juridiques. Elle dit que si le droit de saisir les tribunaux était supprimé et que le RAL était contraignant, il faudrait alors préserver des possibilités de recours bien définies. Elle précise également que les procédures en ligne réclament des systèmes souples, libres des sauvegardes exigées dans les procédures judiciaires.

M. Michael Geist, Professeur à la Faculté de droit de l'Université d'Ottawa (*University of Ottawa Law School)*, déclare qu'il est possible d'établir une liste d'éléments nécessaires au bon fonctionnement du RAL, mais qu'il convient d'aboutir à un compromis sur certaines questions, notamment celles de priorité et de coût. Il dit qu'il faut établir des priorités et que, une fois que certaines décisions auront été prises, il sera important de demander des avis juridiques. C'est actuellement le cas en ce qui concerne les litiges relatifs aux noms de domaines. Quant à la question de savoir qui doit payer le RAL, il ajoute que les sommes investies dans ces systèmes à ce stade sont très modiques, le marché n'étant pas encore réceptif.

M. Matthias Blume, du Ministère de la Justice autrichien, observe qu'il n'est pas facile de distinguer entre ceux qui assument les coûts du RAL et ceux qui respectent les normes. Il juge important de développer la confiance des consommateurs ; à cet égard, les normes ne devraient pas être obligatoires et le caractère volontaire des modes alternatifs de règlement des litiges devrait être

préservé. S'agissant des programmes de labellisation des RAL, il estime que des mesures d'application sont nécessaires et explique que des mesures de ce type ont été instaurées en Autriche.

Mme Jean Ann Fox signale que lorsque les consommateurs achètent des produits en ligne, ils lisent rarement l'accord de RAL et n'acceptent donc pas volontairement d'être liés par ses termes. Elle précise qu'elle est fermement opposée à la proposition de M. Plesser d'exiger des consommateurs qu'ils se plient à la procédure de RAL avant de saisir les tribunaux. Elle estime que les modes alternatifs de règlement des litiges doivent être mis en place de manière à paraître plus intéressants aux consommateurs que les tribunaux.

M. Plesser répond qu'il faut justifier le coût des modes alternatifs de règlement des litiges. Il dit que sa proposition d'épuisement des recours est une solution de compromis, qui n'empêche pas la saisine des tribunaux mais demande simplement qu'une procédure de RAL soit d'abord tentée.

M. Blume déclare qu'en trois ans d'activité dans le domaine de la consommation, il n'a jamais vu un consommateur saisir les tribunaux en première instance. Il soutient toutefois l'idée que les consommateurs doivent pouvoir intenter un procès à tout moment pendant un litige.

M. Hubert van Breemen explique que dans le système néerlandais, les décisions contraignantes sont possibles mais qu'y recourir est décidé en commun par les représentants des entreprises et des consommateurs.

Une autre question est posée dans la salle au sujet du maintien des actions collectives en justice dans le cadre du RAL. M. Plesser décrit ses actions et explique que dans certaines de ces affaires, aux États-Unis, des courtiers en valeurs ont opté pour l'arbitrage obligatoire.

M. Mozelle Thompson clôt la session en soulignant qu'il est nécessaire d'encourager les représentants des entreprises et des consommateurs à travailler en collaboration sur ces questions juridiques.

Session 5-III : Principe de la décision en dernier ressort et juge d'appui

Thème : Cette session avait pour objet d'étudier l'interface entre les RAL en ligne et le cadre juridictionnel, pendant les procédures RAL et dans les cas où ils échouent.

Mme Catherine Kessedjian, Professeur à l'Université de Paris II, remplit les fonctions de modérateur au cours de la 3e séance de la session 5.

Elle présente les grands thèmes de la session, qui doit tout d'abord examiner si le recours à un *juge d'appui*, notion qui existe dans le cadre de l'arbitrage des affaires de commerce international, peut faciliter le bon fonctionnement et l'aboutissement d'une procédure RAL, et ensuite la notion de dernier recours, qui préserve le recours aux tribunaux. Mme Kessedjian rappelle que la session est axée sur la méthodologie et les compétences du juge et n'aborde pas les questions relatives au droit applicable.

Elle invite les panélistes à débattre du rôle éventuel du *juge d'appui* dans les RAL.

M. Roger Cochetti, Premier Vice-président et Responsable de l'analyse stratégique à VeriSign, répond que le concept de *juge d'appui* est utile mais se fonde sur l'hypothèse que les litiges sont peu nombreux et portent sur des sommes élevées, hypothèse qui sous-tend la pratique de l'arbitrage

commercial international. Dans le cadre du commerce électronique, il estime que cette hypothèse n'est pas défendable dans la mesure où, le plus souvent, les litiges sont nombreux mais portent sur de faibles montants. Il ajoute qu'il serait difficile d'intégrer un processus judiciaire dans le RAL sans porter atteinte au principe selon lequel la procédure doit être économique pour les deux parties.

M. David Goddard, avocat représentant le Commissariat du droit néo-zélandais, expose quatre situations fondamentales où le juge peut s'avérer utile dans le cadre du RAL : i) application pure et simple des droits des consommateurs puisque les tribunaux détiennent toujours l'exercice exclusif des pouvoirs de coercition ; *ii)* en qualité de juge de dernier recours, en disposant de règles claires pour le cas où un RAL échouerait ; *iii)* en qualité de juge d'appui, dans les cas d'arbitrage obligatoire (dans les cas d'arbitrage non obligatoire où les parties ne parviennent à se mettre d'accord sur une procédure RAL de remplacement, il n'y a guère d'espoir qu'un accord soit possible sur le fond) ; *iv)* dans l'application exécutoire d'un règlement.

Mme Naja Felter, de Consumer International, affirme que les consommateurs devraient toujours pouvoir saisir les tribunaux et ne jamais avoir à renoncer à ce droit. Elle convient que le concept de juge d'appui est difficile à intégrer aux transactions entre entreprises et consommateurs compte tenu du faible montant sur lequel portent habituellement les différends. Elle ajoute que si les modes alternatifs de règlement des litiges sont convenablement supervisés, il ne devrait pas être besoin de recourir à un juge d'appui.

Mme Asuncion Capparros, Directeur des affaires européennes de ABN Amro Bank, dit que le *juge d'appui* constitue un niveau supplémentaire qui n'est pas *a priori* le bienvenu dans le domaine entreprises-consommateurs. Elle soulève par ailleurs la question de l'expérience d'un juge dans ce contexte et de ses qualifications éventuelles. Un juge viendrait-il d'un tribunal ou d'un organisme officiel d'application de la loi ? Dans quel domaine les juges devraient-ils être spécialisés ?

M. Giacinto Bisogni, expert national aux services juridiques de la Commission européenne déclare que, compte tenu de la nature volontaire du RAL, il ne voit pas quel rôle un *juge d'appui* pourrait jouer au cours d'une procédure RAL. Il ajoute que le recours à un juge durant une procédure de RAL risque d'introduire une rigidité excessive. Il propose que la responsabilité de faciliter le bon fonctionnement et l'aboutissement d'une procédure RAL incombe aux prestataires de services RAL ou à un organisme de surveillance.

Un membre du public souligne que les questions de droit applicable et de procédure pourraient être résolues par le juge puisque le tiers neutre n'a aucun pouvoir à cet égard. Il suggère par ailleurs que le rôle du juge pourrait être de protéger les droits des consommateurs dans le cadre de mesures provisoires et protectrices comme dans le cadre de l'application exécutoire des décisions. Il demande en outre s'il ne serait pas approprié, plutôt que d'attribuer un rôle limité à un *juge d'appui* dans la procédure de RAL, de faire en sorte que les juridictions compétentes s'orientent davantage sur la médiation.

Mme Kessedjian invite alors les panélistes à examiner les questions suivantes au sujet du dernier recours : *i)* quel rôle doit jouer un juge ; *ii)* qui devrait être ce juge, quelles sont les compétences requises ; *iii)* le consommateur devrait-il obligatoirement faire un choix ou bien devrait-il y avoir des règles par défaut ; *iv)* quels moyens employer.

M. Goddard donne un aperçu des travaux en cours de la Conférence de La Haye de droit international privé qui portent sur une Convention concernant la compétence judiciaire et l'exécution des jugements étrangers. La proposition initiale de la convention d'établir une compétence judiciaire spéciale pour les consommateurs (c'est-à-dire le lieu de résidence habituel du consommateur) a

soulevé une vaste controverse. Compte tenu de la complexité du problème, certains ont proposé d'exclure les consommateurs du champ d'application de la Convention ; d'autres ont proposé que les pays soient autorisés à laisser leurs consommateurs accepter d'autres instances que celles prévues par la Convention. Une autre possibilité serait de conserver la compétence judiciaire traditionnelle (le lieu de résidence habituel du défendeur, le lieu de l'établissement ou de sa succursale, le lieu où le délit civil a eu lieu, ou la comparution volontaire du défendeur).

Mme Caparros rappelle que si, aux termes de la législation européenne en vigueur, les consommateurs ont le droit de saisir les tribunaux dans leur pays de résidence, ils peuvent avoir besoin de chercher à obtenir l'application exécutoire d'un jugement dans un pays étranger.

M. Cochetti signale que l'accès des consommateurs aux tribunaux locaux n'est pas pragmatique et que les décisions seront probablement inexécutables compte tenu des faibles sommes sur lesquelles portent les litiges.

Enfin, M. Giacinto Bisogni rappelle que la Commission envisage une consultation générale sur la création d'un espace extrajudiciaire européen où les décisions issues des procédures RAL seraient exécutoires.

Un membre du public souligne qu'il est important de concevoir des règles qui ne découragent pas les plus petits pays et les secteurs d'activité moins importants de participer au commerce électronique.

Session 5-IV : Problèmes technologiques liés aux RAL en ligne

Thème : Cette session devait mettre en évidence les technologies déjà utilisées ou en développement afin de montrer comment elles peuvent contribuer à faciliter le règlement des différends en ligne entre les entreprises et les consommateurs. Ainsi, les technologies servant à protéger la signature et l'authentification électroniques, ou le chiffrement des messages, peuvent contribuer à assurer la confidentialité et l'intégrité de la procédure et de l'information échangée. Par ailleurs, grâce aux techniques interactives, telles que la visioconférence, les parties peuvent se rassembler en un même lieu virtuel, au lieu de rester derrière leur écran informatique, et l'interaction se fait face-à-face. De même, la traduction automatique et la reconnaissance vocale permettent de surmonter certaines différences culturelles.

M. Wibo Koole, Chef du Département de la politique à l'égard des consommateurs du Consumentenbond NL, assume le rôle de modérateur pour la 4e séance de la 5e session. Il souligne qu'il convient d'examiner en quoi la technologie peut appuyer le RAL et accélérer son développement.

M. Chris Lynn, Avocat conseil de Microsoft Europe, Afrique et Moyen-Orient, fait un exposé sur les progrès technologiques qui seront utiles au RAL en ligne. Il axe son analyse sur les progrès dans le domaine des langages informatiques, sur la visioconférence évoluée et sur les logiciels de traduction et de reconnaissance vocale. M. Lynn souligne que la technologie est neutre du point de vue déontologique et que les usagers doivent réfléchir aux questions stratégiques avant de déployer des systèmes.

Il décrit le XML (extensible markup language), un langage qui permet aux applications Internet de communiquer entre elles et de prendre des décisions « intelligentes » à partir des informations échangées. Le XML connecte tous les composants techniques de la chaîne de distribution. Dans le contexte du RAL, il fait observer qu'il pourrait contribuer à la transparence en aplanissant certains obstacles interpersonnels, par exemple en autorisant des « poignées de mains » numériques à titre de signature. Il évoque les techniques d'accès à large bande ultrarapides comme Mbone, qui offriront un outil de visioconférence sûr, de haute qualité, à coût modique. Enfin, M. Lynn parle des progrès des

logiciels de traduction et de reconnaissance vocale. Bien que les versions disponibles soient loin d'être parfaites, les logiciels « intelligents » en cours de développement promettent de modifier la perception des usagers.

M. Joseph Alhadeff, Vice-président, Politique publique mondiale, Oracle, entame ensuite une analyse des questions politiques à prendre en compte lors de la mise en place d'un RAL en ligne, notamment comment les prestataires de RAL utilisent la technologie et en quoi celle-ci influence l'évaluation des faits par l'arbitre. Les parties qui effectuent des transactions en ligne doivent notamment se poser les questions suivantes : *i)* pouvez-vous authentifier l'autre partie (sont-ils véritablement ce qu'ils prétendent être ?) ; *ii)* en tant que cybermarchand, quelles sont mes obligations fiscales lorsque je fournis des biens et des services transfrontières ? ; *iii)* avec qui les informations relatives aux consommateurs ont-elles été partagées (y a-t-il des problèmes de vie privée ?).

M. Alhadeff discute également les questions techniques spécifiques au service à la clientèle en ligne, notamment : la navigabilité d'un site Web et les fonctionnalités linguistiques ; la sécurité et la confidentialité des données en ligne ; la possibilité pour un commerçant de connaître la disponibilité d'un produit. Pour les prestataires de RAL, il souligne qu'il convient d'effectuer régulièrement des copies de sauvegarde des systèmes afin de préserver l'intégrité des données. Enfin, il recense plusieurs obstacles d'ordre technique et politique à la confiance des consommateurs. Du point de vue technique, on peut citer les problèmes d'usurpation d'identité, de sécurité des informations relatives aux cartes de paiement et l'absence de contrôle dont dispose le consommateur. Côté politique, on peut mentionner la protection de la vie privée, l'authentification, la fraude et la protection des consommateurs.

Débat

- Les techniques commerciales habituelles peuvent être employées dans le cadre des RAL en ligne. Le XML et les autres techniques nouvelles, comme la visioconférence, seront utilisées ultérieurement. Du fait que le XML peut servir à régulariser un groupe d'applications, il pourrait faire fonction de langage étendu de règlement des litiges. Dans un premier temps, il serait peut-être nécessaire de disposer d'une technologie intermédiaire simple, non pas une Cadillac mais une technique de « transport public » (M. Peter Lubkert, Chef de la Division Technologies de l'information et des réseaux, OCDE).
- Des problèmes linguistiques risquent toujours de surgir au cours d'une visioconférence, tandis que les communications asynchrones donnent à chaque partie le temps de comprendre pleinement les textes qu'elles lisent et qu'elles envoient. (Mme Pippa Lawson).
- Il faut établir des normes et des critères génériques pour le RAL. L'enjeu consiste à les traduire en normes technologiques. Il semble qu'un niveau d'automatisation très élevé soit nécessaire pour gérer les premières étapes d'un règlement des litiges en ligne, la négociation directe par exemple. (M. Marc Wilikens, Centre de recherche commun de la Commission européenne).
- La technologie doit être guidée par des principes car, d'un côté, les outils techniques peuvent aider les consommateurs à préserver leur anonymat en ligne et, de l'autre côté, la technologie représente aussi une menace pour la protection des données et les libertés individuelles. Le RAL risque de ne pas convenir aux litiges portant sur la vie privée où les usagers doivent obtenir un redressement par voie d'injonction. Comme la plupart des violations de la vie privée ne sont pas des cas isolés, mais sont perpétrées à l'encontre d'un grand nombre d'usagers, il faut maintenir le droit à des actions collectives en justice (Mme Sarah Andrews, analyste des politiques, EPIC/Privacy International)

Mme Susan Grant, Directeur du Centre national d'information sur la fraude (*National Fraud Information Center*) de la Ligue nationale des consommateurs (*National Consumers League*), prend la parole depuis la salle pour soulever la question de l'interopérabilité du matériel et des logiciels informatiques entre le prestataire de RAL et le consommateur. Elle propose une approche similaire à celle adoptée par la loi sur la signature électronique récemment votée aux États-Unis, qui exige que les consommateurs donnent leur consentement à recevoir des documents électroniques d'une manière qui prouve que les systèmes dont ils sont équipés peuvent recevoir ces informations.

Au cours d'un bref débat sur les agents logiciels « intelligents », M. Alhadeff s'inquiète de ce que, bien qu'utiles, ces agents pourraient créer des difficultés juridiques s'ils prennent des décisions de la part des parties.

Session 6 : Le rôle des acteurs

Thème : A partir des discussions précédentes, cette dernière session était destinée à mettre en évidence l'opinion partagée par les acteurs sur divers éléments socio-économiques, juridiques ou technologiques que devrait comporter tout RAL en ligne équitable et efficace pour les litiges entre entreprises et consommateurs. Les participants devaient tenter de définir le meilleur moyen de favoriser leur mise en œuvre en explorant deux grands domaines d'action.

Arie van Bellen, Directeur général de Electronic Commerce Platform Nederland, assume les fonctions de modérateur de la 6e Session.

Session 6-I : Promouvoir la loyauté et l'efficacité des RAL en ligne et assurer la bonne mise en œuvre (par exemple, programmes de labellisation et de certification)

Thème : Cette session devait poursuivre le débat sur le rôle des acteurs dans la promotion des RAL entreprises-consommateurs en ligne équitables et efficaces. Il s'agissait de discuter comment les acteurs devraient coopérer pour identifier les éléments essentiels des RAL en ligne (par exemple : qui doit siéger ? Les différents acteurs doivent-ils formuler des recommandations différentes, comme c'est actuellement le cas ? Sur quelles règles se fonder pour les RAL, une réglementation ou des codes de conduite ?). Il s'agissait également de définir comment les acteurs peuvent œuvrer ensemble au respect de ces éléments.

M. Naoshi Shima, Vice-président du Développement de l'activité Internet chez NEC Corporation, expose les grands traits du système de règlement des litiges au Japon. Il signale que si la plupart des consommateurs japonais ont confiance en la bonne foi des cybermarchands, ils sont très sévères en ce qui concerne les défauts des produits et services. Les normes de qualité sont donc plutôt élevées. Les consommateurs peuvent avoir recours aux tribunaux, mais la plupart préfèrent négocier directement avec le cybermarchand ou utiliser les modes alternatifs de règlement des litiges comme la consultation et la médiation si la négociation directe échoue.

La loi japonaise relative à la protection des consommateurs oblige les pouvoirs locaux à établir des centres de consultation pour les litiges entreprises-consommateurs. Par ailleurs, les ONG et les associations professionnelles gèrent des centres de consultation. Presque tous les litiges dont sont saisis les centres sont réglés. Ceux-ci opèrent hors ligne et n'ont pas les connaissances et les compétences nécessaires pour fonctionner en ligne. M. Shima évoque plusieurs questions relatives au règlement des litiges qui font l'objet d'un débat au Japon, notamment la déréglementation de la « loi relative aux avocats », qui autorise les seuls avocats à traiter les litiges dans le domaine de la consommation.

Mme Barbara Wellbery, Associée, Morrison & Foerster, LLC, présente son point de vue sur le rôle des acteurs dans la définition des critères applicables aux modes alternatifs de règlement des litiges en ligne. Elle observe qu'à ce stade, les acteurs conviennent que le RAL doit être efficace, gratuit ou peu onéreux pour les consommateurs, aisément disponible, indépendant et impartial. Elle se demande toutefois combien de temps ce consensus durera une fois qu'ils auront commencé à discuter les caractéristiques de chacun de ces éléments. Elle cite une situation similaire, surgie lors de discussions sur les principes de vie privée dans le cadre de l'accord Safe Harbour récemment adopté entre les États-Unis et l'Union européenne. Elle énumère par ailleurs plusieurs aspects du RAL sur lesquels les participants ne sont pas encore d'accord : qui doit assumer le coût du RAL ; les compromis éventuels entre garanties procédurales et efficacité ; si le RAL peut être obligatoire pour les consommateurs ; si les décisions issues de la procédure RAL peuvent être exécutoires pour les consommateurs.

Elle analyse deux possibilités en ce qui concerne qui devrait établir les règles du RAL : les autorités publiques ou le secteur privé. Elle défend l'idée que, les gouvernements ayant des intérêts et des points de vue nationaux, il est peu probable qu'ils adoptent des lignes directrices compatibles dans le monde entier. Elle recommande plutôt que le secteur privé prenne les rênes en vue d'établir des critères pour le RAL en ligne, en s'assurant que tous les acteurs participent à ce processus. Elle suggère par ailleurs que si les acteurs limitent l'exercice à l'établissement de règles applicables aux RAL transfrontières en ligne pour les transactions entreprises-consommateurs et aux litiges simples portant sur la vie privée, la tâche sera plus raisonnable.

M. Malcolm Crompton, Commissaire à la protection de la vie privée de l'Australie, présente la démarche co-réglementaire proposée par l'Australie pour la protection de la vie privée. La loi australienne en la matière prévoit soit l'établissement de codes de conduite sectoriels et d'organismes connexes de réclamations chargés de régler les différends, soit l'habilitation du commissaire pour la protection des données à traiter les réclamations des consommateurs. La démarche consiste à fixer des normes et des références minimales pour la protection de la vie privée, et de permettre au marché de mettre au point des solutions conformes ou supérieures à ces normes. Le Commissariat à la protection de la vie privée appliquera les normes et veillera à leur respect. M. Crompton précise que les Australiens effectuent 50 % de leurs transactions avec l'étranger, où les lois nationales ne s'appliquent pas. C'est pourquoi il est important que les commissaires pour la protection des données collaborent à l'échelle mondiale. Il cite l'exemple d'une étude récemment conduite conjointement par son bureau et par celui du Commissaire à la protection de l'information et de la vie privée de l'Ontario (Canada) sur les programmes de labellisation en ligne. Il appelle les commissaires à repenser leur rôle à l'ère Internet, en l'axant sur la coopération et les partenariats stratégiques.

M. Martin Bond, Assistant du directeur, Ministère du commerce et de l'industrie du Royaume-Uni (*UK Department of Trade and Industry)*, expose la démarche adoptée par le Royaume-Uni pour définir le rôle des acteurs dans l'établissement de règles régissant le commerce électronique. Il dit qu'il existe une demande de cautionnement officiel et que les gouvernements peuvent contribuer à forger des liens à l'échelle mondiale. Il décrit la méthode « allégée » du Royaume-Uni pour réglementer l'élaboration de codes de bonne pratique et de programmes des meilleures pratiques. Il encourage vivement les organisations de consommateurs à participer à ce processus afin que tous les acteurs s'y rallient.

M. Bond présente le programme TrustUK, par l'intermédiaire duquel le gouvernement britannique encourage la mise en place de codes de conduite. Plutôt que d'imposer un code unique à l'environnement en ligne, TrustUK approuve des codes de bonne pratique qui intègrent des normes fondamentales, par exemple en matière de vie privée, de publicité et de communication d'informations contractuelles. Il souligne que le RAL devrait faire partie intégrante de ces systèmes.

Il remarque que grâce à ce système, le gouvernement est bien placé pour encourager la création de liens entre les codes nationaux. Par exemple, TustUK participe aux travaux de groupe des parties prenantes de la CE qui cherchent à élaborer des lignes directrices destinées aux fournisseurs de codes en Europe. Il mentionne aussi des instances comme l'OCDE où les gouvernements peuvent participer à l'échelle internationale.

Débat

- Les gouvernements ont un rôle important à jouer dans l'établissement d'un cadre politique général. Ils devraient notamment fixer des lignes directrices pour des systèmes de RAL équitables et fiables et pour faciliter la coopération internationale dans ce domaine, par exemple pour encourager la reconnaissance mutuelle de programmes de labellisation en ligne. (M. Yuko Yasunaga)
- On assiste à une multiplication des programmes de labellisation et de RAL au niveau national, et des lignes directrices générales sont nécessaires, qui devraient s'appliquer à tous les types de différends. Il est important que les prestataires de RAL, qui ont une expérience pratique du traitement des litiges, participent à leur élaboration. (Mme Rebecca Richards, Directeur, Politique et harmonisation de TRUSTe)
- S'agissant de l'élaboration de lignes directrices, les autorités publiques devraient procéder avec prudence car ils ont tendance à être trop territoriaux. L'Internet est en phase liminaire de développement, étant donné que plus de 50 % des sites Web actifs ont été lancés cette année seulement et que plus de la moitié des consommateurs qui dépensent de l'argent en ligne l'ont fait pour la première fois cette année. Toutefois, l'adoption d'une démarche prudente ne signifie pas inaction. (M. Roger Cochetti)
- S'il est vrai que l'Internet est en phase liminaire de développement et que des expérimentations sont nécessaires, quelques recommandations s'imposent à ce stade. Des lignes directrices devraient être données à haut niveau, à l'instar des lignes directrices sur la protection des consommateurs de l'OCDE. Les participants devraient réfléchir au rôle des acteurs. Les organisations de consommateurs, par exemple, peuvent donner des informations aux entreprises et évaluer leurs services, comme elles l'ont fait dans le cas de la liste de contrôle des cyberachats pour les consommateurs établie par le Dialogue transatlantique avec les consommateurs. (Mme Susan Grant)
- L'adoption de lignes directrices ne devrait pas être reportée sous prétexte que le marché est en développement ; une fois que les systèmes en ligne seront établis, les entreprises pourront soutenir qu'il est trop onéreux de les modifier pour intégrer les nouvelles normes. (Mme Jean Ann Fox)

M. David Mair explique qu'il est difficile de savoir qui s'exprime véritablement au nom du commerce électronique dans le cadre des discussions des parties prenantes. Ainsi, il n'est pas toujours facile d'entendre les arguments des détaillants et des PME. M. David Mair déclare également qu'il est important de distinguer nettement les deux points suivants : *i)* le rôle de la technologie dans le RAL ; *ii)* le rôle du RAL dans le commerce électronique. Il souligne qu'il convient de faire très attention à ne pas brouiller la distinction entre ces deux questions et de les traiter séparément.

Thème : Les RAL transfrontières sont monnaie courante d'entreprise à entreprise (B-to-B), mais c'est un phénomène nouveau entre entreprises et consommateurs.Conscients du fait que les utilisateurs et les consommateurs connaissaient et comprennent mal ces systèmes, les participants à cette session devaient se concentrer sur le rôle des divers acteurs dans la sensibilisation des consommateurs et des entreprises aux mécanismes de règlement des litiges en ligne. Le débat devait notamment porter sur les moyens permettant de sensibiliser efficacement les entreprises à l'offre de RAL et de renseigner les consommateurs sur la nature des RAL équitables et efficaces et sur les procédures y afférentes.

M. Francis Aldhouse, Adjoint au Commissaire pour la protection des données (Royaume-Uni) explique brièvement le rôle de la Commission pour la protection des données et la loi sur la protection des données de 1998. Il explique que la loi est appliquée par le biais de poursuites pénales et ajoute qu'il y a obligation de vérifier qu'elle est respectée sur la demande de tout individu. Toutefois, le principal mode d'application est l'octroi d'une période de préavis, il s'agit donc en quelque sorte d'un pouvoir réglementaire. M. Aldhouse argumente toutefois que la meilleure façon de progresser n'est pas de confier un rôle de contrôle à la Commission mais plutôt de provoquer un changement culturel, par exemple en obtenant des sociétés qu'elles incluent la protection de la vie privée dans leurs plans d'entreprise et en encourageant les bonnes pratiques, notamment le RAL.

La Commission sur la protection des données reçoit entre 5 et 6 000 réclamations par an. M. Aldhouse signale que l'année dernière, deux tiers des affaires qu'elle a traitées portaient sur de simples litiges factuels. Il évoque également les efforts de la Commission pour informer les consommateurs de leurs droits en matière de vie privée, ce qu'elle fait par des campagnes de publicité télévisées et d'affichage.

Mme. Grant renvoie les participants à la conférence au site Internet de la Consumers League (www.nclnet.org). Elle signale que le site propose un guide du cyberachat en toute sécurité et ajoute qu'une sensibilisation efficace du public est un élément primordial.

M. Mair observe qu'il est important d'étudier le RAL dans un cadre plus vaste. Il dit qu'il faut informer les consommateurs que si une transaction se passe mal, un système performant de traitement des réclamations est disponible, qu'ils peuvent ensuite avoir recours au RAL et enfin, si ces procédures ne suffisent pas à leur donner réparation, qu'ils peuvent saisir les tribunaux.

M. Yasunaga signale que les consommateurs qui ne connaissent pas les programmes de labellisation ou les problèmes du cyberachat sont les plus susceptibles de rencontrer des difficultés. Il dit qu'il est important de faire connaître les RAL et que les représentants des consommateurs devraient jouer un rôle plus actif dans ce domaine. Il précise que les jeunes générations sont plus réceptives aux campagnes d'informations que les adultes.

M. Cochetti convient que la sensibilisation est un élément extrêmement important. Il évoque un projet de protection de la vie privée qui lance actuellement, aux États-Unis, une campagne d'information sur la protection de la vie privée sur l'Internet. Il annonce que sa société est en train d'élaborer un programme d'information destiné aux PME sur les codes de bonne conduite et d'autres systèmes d'autoréglementation.

Mme Richards déclare qu'il ne faut pas perdre de vue la nécessité d'informer les acteurs hors ligne comme en ligne.

Conclusions de la conférence

M. Ford récapitule les principaux thèmes débattus le premier jour :

- Les discours d'ouverture ont mis en lumière le besoin de partenariats mondiaux entre les différents acteurs ; c'est un aspect crucial de l'élaboration de modes alternatifs de règlement des litiges en ligne équitables et efficaces pour les différends entre entreprises et consommateurs. Les orateurs ont également reconnu les défis juridiques et technologiques complexes qui doivent être relevés pour atteindre cet objectif.
- La première session a présenté une synthèse des travaux en cours pour mettre en place des RAL en ligne aux niveaux national, régional et international. Il en est clairement ressorti que les parties prenantes – autorités publiques, entreprises et organisations de consommateurs – manifestent un engagement identique à promouvoir le RAL pour résoudre les litiges entre entreprises et consommateurs. Le débat a permis de cerner les terrains d'entente et les divergences à surmonter entre les différents acteurs en ce qui concerne les aspects essentiels du RAL en ligne. Un certain consensus s'est dégagé dans quelques domaines. Chacun a reconnu qu'il convenait de trouver le moyen d'éviter les litiges entre entreprises et consommateurs. Il est évident à ce stade qu'un modèle unique de RAL ne peut convenir à tous les types de litiges. Ensuite, étant donné la nature sans frontières de l'Internet, les modes alternatifs de règlement des litiges doivent être conçus de manière à surmonter les différences culturelles. Enfin, s'il est crucial que les RAL soient équitables et efficaces, la vitesse de la prise de décision devrait être adaptée à l'Internet. Les exposés présentés au cours de cette session ont aussi mis en lumière les domaines à explorer plus avant, notamment les questions relatives au choix du consommateur (RAL volontaire ou obligatoire), au caractère contraignant ou pas des décisions, à la conformité et à l'exécution.
- La session 2 a présenté des débats et des statistiques sur les types les plus fréquents de litiges entreprises-consommateurs en ligne et sur les taux de conformité aux réglementations relatives à la protection de la vie privée. Les réclamations les plus fréquentes des consommateurs portent sur le non-livraison des produits, suivie de leur livraison tardive, puis des problèmes associés aux coûts. Certaines des réclamations sur la vie privée les plus communes concernent les courriers électroniques commerciaux non sollicités, l'usurpation d'identité, le harcèlement téléphonique, la fourniture d'informations sur la solvabilité sans le consentement de l'intéressé, la vente de données à des tiers et la protection de la vie privée des enfants. Un nombre croissant de réclamations relatives au commerce électronique porte sur des transactions transfrontières. L'importante de la coopération dans le domaine de l'application des lois a également été mise en valeur par la présentation d'une base de données commune des États-Unis et du Canada qui recense les réclamations portant sur des fraudes.
- La session 3 s'est concentrée sur l'attente des consommateurs en termes de service et sur les mécanismes de remboursement par carte de paiement comme moyen de régler les différends. Des études récentes montrent que les consommateurs attendent des réponses plus rapides des cybermarchands et sont moins susceptibles de rester fidèles si les problèmes ne sont pas traités par des mécanismes internes. Il est important d'informer les cybermarchands des besoins des consommateurs. Un point essentiel évoqué au cours de cette session est que les remboursements ne sont pas une forme de RAL mais constituent un élément important dans le règlement des litiges de consommation.

- La session 4 a permis d'entendre des communications et des débats sur les différents types de modes alternatifs de règlement des litiges en ligne, notamment les systèmes automatisés (où la décision est rendue par un ordinateur) : la négociation directe et la médiation : les systèmes d'arbitrage officiels : les systèmes transfrontières en développement. Bien qu'on ne sache pas précisément quels systèmes RAL conviennent le mieux à la résolution de différents types de litiges, les participants se sont accordés sur le fait que les systèmes automatisés actuels sont essentiellement conçus pour résoudre des litiges pécuniaires. Il a été reconnu qu'il y a des limites à ce que les RAL peuvent accomplir, que leur développement est encore en phase initiale, mais qu'ils offrent un grand potentiel.
- La session a aussi souligné la nécessité de former des tiers neutres et des intermédiaires et de sensibiliser les parties prenantes. Les participants ont examiné plusieurs difficultés que présentent les systèmes en ligne pour les consommateurs ; l'asymétrie de l'information, les obstacles linguistiques, le financement des mécanismes et le lien entre le financement et l'impartialité du système de RAL.

Mme Ølgaard récapitule les thèmes essentiels discutés au cours de la deuxième journée :

- La session 5-I a étudié les différences culturelles dans le cadre du règlement des litiges et les aspects économiques du RAL en ligne. Il est clairement apparu qu'il ne s'agit pas seulement de tenter de venir à bout des obstacles linguistiques, mais aussi des différences culturelles qui influencent la résolution des litiges, par exemple les habitudes des consommateurs en matière de réclamation et leurs attentes en termes de service à la clientèle et de RAL.
- S'agissant de l'aspect économique du règlement des différends, il a été souligné que certains litiges peuvent être trop onéreux pour être résolus par un RAL en ligne, et qu'offrir un RAL à coût modique aux consommateurs soulève la question de savoir qui doit en assumer le coût. Doit-il être assumé par l'ensemble des consommateurs, alors que tous n'ont pas de litiges, ou bien la concurrence serait-elle assez intense pour entraîner une baisse du prix global ? Un autre enjeu est que le besoin d'efficacité économique risque de contredire la nécessité de développer la confiance du consommateur. Il faut encore travailler à établir un équilibre entre ces deux éléments.
- La session 5-II s'est essentiellement attachée aux questions épineuses du recours volontaire ou obligatoire à l'ADR, notamment l'idée d'un impératif d'épuisement des recours pour les consommateurs avant de saisir les tribunaux, et du caractère contraignant ou non contraignant des décisions. La session n'a pas abouti à des solutions concrètes, mais elle a clairement établi que des travaux dans ce domaine sont nécessaires, à commencer par des définitions terminologiques. Le RAL oblige les acteurs à se pencher sur certains aspects fondamentaux du système juridique.
- La session 5-III a vu un consensus se dégager sur le fait que le recours à un *juge d'appui*, s'il est valable en théorie, n'est peut-être pas réalisable dans la pratique sauf, éventuellement, dans un nombre limité de cas. En fait, les participants ont craint que cela n'alourdisse la procédure en ajoutant un niveau de compétence. Le principe de dernier recours doit faire l'objet de travaux approfondis, notamment sur le mode de sélection de l'instance compétente.
- La session 5-IV a souligné que la technologie est essentielle au RAL en ligne mais nécessite un cadre politique général pour garantir la sécurité et la confidentialité d'une part, la transparence et la simplicité d'autre part. Les progrès accomplis en termes de normes techniques – le XML par exemple – offrent l'occasion d'harmoniser et de développer l'interopérabilité des RAL à l'échelle mondiale. De même, les progrès technologiques –

logiciels de traduction, agents intelligents, visioconférence – peuvent améliorer l'efficacité des RAL et la possibilité de réunir des parties de quelque endroit que ce soit au monde en un dialogue face-à-face.

Bien que la technologie du RAL en ligne soit très prometteuse, comme dans d'autres domaines du commerce électronique, les participants ont signalé que des problèmes d'atteinte à la vie privée continuent de surgir et qu'il faut continuer à les examiner à mesure que la technique évolue. De même, certains avantages de la technologie peuvent également entraîner des choix difficiles. Ainsi, alors que certains usagers pourraient privilégier des mécanismes de règlement face-à-face, la communication asynchrone permet à une partie de délibérer plus longuement sur la réponse à donner.

- Les participants à la session 6 ont exprimé leurs points de vue sur le rôle approprié des acteurs dans le développement des RAL en ligne. Les organisations de consommateurs savent précisément ce qu'elles pourraient apporter au processus. La consultation avec les groupes de consommateurs ne devrait pas se limiter à écouter leurs opinions, mais aussi les intégrer dans les projets. Certains ont estimé que les autorités publiques devraient être impliqués dans la mesure où ils peuvent inspirer confiance et légitimer démocratiquement une discussion des divers aspects du RAL. D'autres ont affirmé que le secteur privé devrait montrer la voie puisque le commerce électronique ne connaît pas de frontières et que les autorités publiques sont circonscrits à leurs frontières nationales. Le secteur privé en appelle à tous les acteurs, dans le monde entier, à tenter de surmonter les obstacles au commerce électronique. Outre l'implication actuelle des entreprises et des représentants des consommateurs et des autorités, l'importance de la participation des autres acteurs a été soulignée. Une représentation plus vaste des prestataires de services RAL et des cybermarchands serait profitable au débat.
- Enfin, il a été convenu qu'une tâche extrêmement importante consistait à diffuser les informations relatives au RAL en ligne et à y sensibiliser les usagers individuels et les entreprises.

Les présidents des sessions remercient les participants de leurs observations et les invitent à diffuser auprès du plus grand nombre les enseignements de la conférence.

APPENDICE A : MÉCANISMES DE RAL EN LIGNE

Service de RAL en ligne	URL	Type(s) de litige réglé (s)	Litiges B-to-B, B-to-C ou C-to-C	Méthode RAL utilisée	Langues	Origine géographique	Source de financement
123Settle	https://ssl-073.imconline.net/123settle/details/Mediation_Init.asp	tous	B-to-B, B-to-C, C-to-C	négociation automatisée : médiation : arbitrage	anglais (espagnol à venir)	États-Unis	commission payée par l'usager
AllSettle	www.allsettle.com/	assurance uniquement	B-to-C	négociation automatisée	anglais	États-Unis	commissions à la société d'assurance
BBBOnline	www.bbbonline.org	tous litiges consommation	B-to-C	conciliation, médiation, arbitrage	anglais	États-Unis/Canada	cotisations des entreprises adhérentes
clickNsettle	www.clicknsettle.com	tous litiges financiers	B-to-C	négociation automatisée	anglais & espagnol	États-Unis	commission payée par l'usager
Cyberarbitrage	www.cyberarbitration.com	noms de domaine ; tous les autres	B-to-C, B-to-B, C-to-C	arbitrage	anglais	Inde	
Cybercourt	www.cybercourt.org	tous litiges en ligne	B-to-B, B-to-C, C-to-C	médiation	anglais et allemand	Allemagne	à déterminer
Cybersettle	www.cybersettle.com	tous litiges financiers	B-to-C	négociation automatisée	anglais & français	États-Unis	commission payée par l'usager
E-Médiation	www.e-mediation.nl	tous	B-to-B, B-to-C, C-to-C	médiation	néerlandais, anglais	Pays-Bas	à déterminer
Consensus Médiation (e-Mediator)	www.consensusmediation.co.uk/index. html	tous litiges en ligne	B-to-B, B-to-C, C-to-C	médiation	anglais	Royaume-Uni	commission payée par l'usager
eResolution	www.disputes.org/eresolution	noms de domaine ; tous les autres	B-to-B, B-to-C, C-to-C	négociation facilitée, médiation, arbitrage	anglais & français	Canada	commission payée par l'usager
European Advertising Standards Alliance	www.easa-alliance.org	litiges liés à la publicité	B-to-B, B-to-C, C-to-C	approches diverses	anglais & français	UE	cotisation des adhérents
Fsm	www.fsm.de	réclamations contre les membres de l'Association	B-to-C	arbitrage	anglais, allemand & français	Allemagne	cotisation des adhérents
iCourthouse	www.i-courthouse.com/main.taf ?&redir=0	tous	B-to-C, B-to-B, C-to-C	arbitrage non contraignant	anglais (français et espagnol à venir)	États-Unis	commission payée par l'usager

Service de RAL en ligne	URL	Type(s) de litige réglé (s)	Litiges B-to-B, B-to-C ou C-to-C	Méthode RAL utilisée	Langues	Origine géographique	Source de financement
iLevel	www.ilevel.com	tous litiges commerciaux	B-to-C	négociation facilitée ; information consommateurs	anglais	États-Unis	cotisations des entreprises adhérentes
InternetNeutral	www.internetneutral.com	tous litiges commerciaux en ligne	B-to-B, B-to-C	médiation	anglais	États-Unis	commission payée par l'usager
Internet Ombudsman (Austria)		tous litiges commerciaux en ligne		médiation, arbitrage	allemand et anglais	Autriche	État/ONG/secteur privé
Internet Ombudsmannen (Sweden)		tous litiges commerciaux en ligne			suédois	Suède	État
IRIS Médiation	www.iris.sgdg.org/mediation	tous litiges commerciaux en ligne	B-to-B, B-to-C, C-to-C	médiation	français	France	
MARS (SuperSettle; Fair□ other)	www.resolvemydispute.com	tous (Fair&Square – en ligne seulement)	B-to-C, B-to-B, C-to-C	négociation automatisée ; médiation ; arbitrage	anglais (espagnol, français, chinois à venir)	États-Unis	commission payée par l'usager
Mediate-Net		litiges familiaux		médiation	anglais	États-Unis	gratuité pendant l'essai
NEWCourtCity.com (Virtual Mediator & On-Line Médiation)		tous litiges financiers	B-to-B, B-to-C, C-to-C	négociation automatisée, médiation, consultation juridique	anglais, espagnol	États-Unis	commission payée par l'usager
NovaForum	www.novaforum.com/main	tous	B-to-B, B-to-C, C-to-C	négociation facilitée, médiation, arbitrage	anglais, français, allemand, portugais, polonais, russe, ukrainien, cantonais, mandarin	Canada	cotisations des entreprises adhérentes
Online Mediators		tous	B-to-B, B-to-C, C-to-C	médiation	anglais	États-Unis	commission payée par l'usager
Online Ombuds Office	www.ombuds.org/center/index.html	tous litiges consommation	B-to-C	médiation, ombudsman	anglais	États-Unis	subventions publiques/privées
OnlineDisputes	www.robindownes.com/OnLineDisputesWebsite/OnLineHomePg.html	tous litiges commerciaux	B-to-C, B-to-B, C-to-C	médiation automatisée	anglais, espagnol	États-Unis	cotisations des entreprises adhérentes
Resolution Forum	www.resolutionforum.org	tous	B-to-C, B-to-B, C-to-C	négociation facilitée, médiation	anglais, espagnol	États-Unis	commission payée par l'usager
SettlementNow		assurance seulement	B-to-C	négociation automatisée	anglais	États-Unis	commission payée par l'usager

Service de RAL en ligne	URL	Type(s) de litige réglé (s)	Litiges B-to-B, B-to-C ou C-to-C	Méthode RAL utilisée	Langues	Origine géographique	Source de financement
SettleOnline	www.settleonline.com	tous litiges financiers	B-to-C, B-to-B, C-to-C	négociation automatisée	anglais, espagnol	États-Unis	commission payée par l'usager
SettleSmart		tous litiges financiers	B-to-C, B-to-B, C-to-C	négociation automatisée	anglais,	États-Unis	commission payée par l'usager
SettleTheCase	www.settlethecase.com/main.html	tous	B-to-B, B-to-C, C-to-C	médiation, arbitrage, procédure sommaire devant jury	anglais	États-Unis	commission payée par l'usager
SquareTrade	www.squaretrade.com	tous litiges en ligne	B-to-C	négociation facilitée, médiation	anglais	États-Unis	cotisations des entreprises adhérentes et commission payée par l'usager
The Virtual Magistrate	vmag.org	tous litiges consommation en ligne	B-to-C	arbitrage non contraignant	anglais	États-Unis	financé par la faculté de droit
TRUSTe	www.truste.org	litiges en ligne respect de la vie privée	B-to-C	conciliation/négociation	anglais	États-Unis	cotisations des entreprises adhérentes
USSettle	www.ussettle.com	tous litiges financiers	B-to-C, B-to-B, C-to-C	négociation automatisée	anglais	États-Unis	commission payée par l'usager
WebAssured	www.webassured.com	tous litiges consommation en ligne	B-to-C	médiation	anglais	États-Unis	cotisations des entreprises adhérentes
Web Dispute Resolutions	www.webdisputeresolutions.com	tous litiges en ligne	B-to-C, B-to-B,	médiation, arbitrage	anglais	États-Unis	commission payée par l'usager
WEBdispute.com	www.webdispute.com	tous litiges commerciaux en ligne	B-to-B, B-to-C	arbitrage	anglais	États-Unis	commission payée par l'usager
Webmediate	www.webmediate.com/	tous	B-to-C, B-to-B, C-to-C	médiation, arbitrage	Anglais	États-Unis	cotisations des entreprises adhérentes et commission payée par l'usager
Which WebTrader	www.which.net/webtrader/	tous litiges consommation en ligne	B-to-C	ombudsman	langue du pays d'accueil	UK, NL, BG, IT, FR, SP, PO	cotisations des membres et des adhérents, autres ?
WIPO	arbiter.wipo.int/domains/index.html	noms de domaine	B-to-B, B-to-C	arbitrage	anglais, français, espagnol	Suisse	commission payée par l'usager

Source: OECD.

APPENDICE B : ÉLÉMENTS PROCÉDURAUX, SUBSTANTIELS ET AUTRES QUE POURRAIENT COMPORTER LES MODES ALTERNATIFS DE RÈGLEMENT DES LITIGES

Le questionnaire suivant a été élaboré à partir d'une étude factuelle des RAL (mécanismes alternatifs de règlement des conflits) existants. Il est destiné à favoriser les discussions et le débat entre les participants à la conférence, dans le cadre de la réflexion sur la diversité des éléments de procédure et de fond que ces mécanismes peuvent comporter.

1. GÉNÉRALITÉS

1.1. Pour quelles transactions des RAL sont-ils proposés ?

Entre entreprises
Entre entreprises et consommateurs
Entre consommateurs)
Entre pouvoirs publics et consommateurs)

1.2. Pour quel(s) type(s) de litiges des RAL sont-ils proposés ?

Enchères
Entreprises-consommateurs – Différends contractuels
Droits d'auteur (copyright)
Litiges sur noms de domaine
Litiges familiaux
Assurance
Litiges sur la propriété intellectuelle
Autres litiges financiers
Préjudice personnel
Autres

1.3. Quel(s) type(s) de RAL est (sont) proposé(s) ?

Négociation automatisée
Négociation assistée (facilitation, conciliation)
Médiation
Médiation-arbitrage ou autre combinaison de RAL traditionnels
Arbitrage
Ombudsman non public
Tribunaux ne relevant pas de l'État
Autres

1.4. Quelle est la nature de l'entité proposant des RAL ?

Entreprise/groupe industriel
Association de consommateurs
Organisation intergouvernementale
Organisme public national
Cabinet d'avocats
Organisme public local
Université
Association d'anciens juges ou juristes (ou autre organisation professionnelle analogue)
Autres

D'autres types d'entités ont-ils été consultés lors de l'élaboration et de la mise en œuvre du programme de RAL ?
Si oui, lesquels (État, groupement de consommateurs par exemple) ?
Quel a été le rôle de ces entités (financement, validation, orientation, recommandation de pratiques) ?
Le service de RAL a-t-il cherché à nouer des partenariats avec une autre entité exerçant la même fonction ?
Le service de RAL s'engage-t-il à se conformer aux lignes directrices régissant les procédures définies par une entité donnée ?
Si oui, quelle est cette entité ?

1.5. Le programme de RAL est-il certifié et/ou bénéficie-t-il d'un label/sceau de garantie ?

Si oui, par qui ?
Quels sont les effets du processus de certification et/ou d'attribution d'un label/sceau de garantie ?

1.6. Coût du RAL pour les parties :

Les RAL sont-ils des services payants ?
Comment ?
Procédure gratuite
Forfait
Coût fonction de la valeur du litige
Coût divisé entre les parties
Autres (coût calculé sur la valeur de la réclamation, par exemple)

1.7. Combien de temps dure un litige en moyenne ?

1.8. Statistiques :

Quel est le nombre de litiges traités ?
Si possible, préciser le nombre de litiges traités par rapport au nombre total de transactions
Quel est le nombre/pourcentage de litiges ayant pu être réglés ?
Si possible, préciser le nombre/pourcentage de décisions donnant lieu à un appel devant un tribunal ou une autre instance ?
Le nombre/pourcentage de décisions posant des problèmes de conformité a-t-il été noté ?

1.9. Quand le programme de RAL a-t-il été élaboré ?

1.10. Aspects socioéconomiques :

Dans quelle(s) zone(s) géographique(s) l'entité proposant des RAL est-elle présente ?
Dans quels pays ce service est-il fourni ?
Dans quelle langue ?
Existe-t-il des limitations concernant les zones géographiques ou les langues dans lesquelles ce service peut être fourni ?
Dans quelle langue la procédure est-elle menée ?
Qui choisit les langues à utiliser dans la procédure RAL, et sur quelle base ?
Les différences culturelles sont-elles prises en compte ?

1.11. A-t-on mené une enquête pour déterminer si le dispositif donne satisfaction aux usagers ?

Si oui, quels sont les résultats ?

2. RÈGLES, NORMES OU LIGNES DIRECTRICES FONDAMENTALES (CODES D'AUTORÉGULATION VOLONTAIRE, NOTAMMENT)

2.1. Sur quoi les RAL reposent-ils ?

Principe d'équité
Règles, normes ou lignes directrices internationales
Règles, normes ou lignes directrices nationales
Autres

3. RÈGLES DE PROCÉDURE

3.1. RAL volontaires/obligatoires et décisions exécutoires/non exécutoires :

Les deux parties recourent-elles aux RAL de leur plein gré ?
La participation au programme RAL est-elle une condition préalable pour qu'une partie puisse porter un litige devant les tribunaux ?
Une clause RAL exécutoire pré-litige figure-t-elle dans l'accord qui oblige les deux parties à accepter la décision du RAL ?
Une clause RAL exécutoire pré-litige figure-t-elle dans l'accord qui oblige l'une des parties à accepter la décision du RAL ?
Les parties sont-elles autorisées à participer à un RAL dont l'issue les engagera toutes les deux en cas de litige ?
Les parties sont-elles autorisées à participer à un RAL qui engagera l'une d'entre elles en cas de litige ?

3.2. Contenu des règles de procédure :

Le RAL ne repose-t-il que sur l'équité et la bonne foi ?
Le RAL prévoit-il que les parties s'entendent pour définir leurs propres règles ?
Le RAL applique-t-il des règles de procédure établies (par exemple, CNUDCI, CCI, ICANN/OMPI, Règlement uniforme des litiges relatifs aux noms de domaine) ?
Le RAL applique-t-il ses propres règles ou des règles de procédure complémentaires des règles établies ?

4. PROCÉDURE

4.1. La procédure se déroule-t-elle :

Entièrement en ligne ?
En ligne et hors ligne ?
Entièrement hors ligne ?
- Par courrier ?
- En face-à-face ?

4.2. Moyens de communication :

Courrier électronique
Formulaires en ligne
Téléconférence
Téléphone
Face-à-face
Autres

4.3. Des services de traduction/d'interprétation sont-ils fournis/disponibles ?

4.4. La procédure est-elle limitée dans le temps ?

4.5. Les parties peuvent-elles être représentées ou se faire assister ?

4.6. Existe-t-il un droit/une possibilité de confrontation ?

4.7. Procédure contradictoire :

Les parties sont-elles tenues de se communiquer le détail de leurs arguments ?
Une partie peut-elle répondre aux arguments avancés par l'autre ?

4.8. Accessibilité et transparence :

A quelles formes de publicité/marketing le programme de RAL recourt-il ?
Comment le programme de RAL se fait-il connaître auprès des parties ?
A quel niveau d'une transaction est-on informé de la possibilité de RAL (page d'accueil, page de confirmation de l'accord de l'utilisateur) ?
De quelle manière ?
Quelles informations sur le RAL sont-elles communiquées ?

5. INTERMÉDIAIRE(S) NEUTRE(S)

5.1. Qui choisit l'intermédiaire neutre ?

Les parties
Le service de RAL

5.2. Les parties peuvent-elles choisir un intermédiaire ou un groupe d'intermédiaires ? Si oui, comment ?

5.3. Sur quelle base l'intermédiaire (les intermédiaires) est-il (sont-ils) choisi(s) ?

Liste soumise par le service de RAL ?
Liste soumise par une autre entité s'occupant de RAL, telle qu'une organisation professionnelle de services de RAL ?
Autres

5.4. Les parties peuvent-elles contester la désignation d'un intermédiaire neutre ? Si oui, comment ?

5.5. Quels domaines un intermédiaire neutre doit-il bien connaître ?

Informatique
Droit
Techniques relatives aux RAL
Compétences liées au sujet du litige
Certification par organisme professionnel
Autres

5.6. Quel est le rôle de l'intermédiaire neutre ?

Il aide les parties à parvenir à un accord
Il évalue les éléments de fond du dossier
Il évalue les éléments de procédure du dossier
Il détermine les recherches à mener
Il propose des mesures provisoires ou d'urgence
Il communique son avis sur l'issue à donner au litige
Il impose une décision
    a) Par écrit
    b) En la motivant

5.7. L'intermédiaire doit-il être impartial ? Si oui, comment cette impartialité est-elle assurée ?

5.8. L'intermédiaire agit-il bénévolement ?

6. CONFIDENTIALITÉ

6.1. L'intermédiaire neutre et le service RAL sont-ils de préserver la confidentialité des aspects suivants ?

Existence de la procédure
Informations échangées pendant la procédure
Issue de la procédure

6.2. Les parties sont-elles tenues de préserve la confidentialité des aspects suivants ?

Existence de la procédure

Informations échangées pendant la procédure
Issue de la procédure

6.3. Quelles informations concernant chaque décision sont-elles rendues publiques (par exemple, communication des données de fait ou uniquement du résultat de la procédure) ? Comment décide-t-on de cette divulgation ?

6.4. Les parties, les intermédiaires neutres et les services RAL sont-ils autorisés à porter devant la justice les réclamations/litiges/décisions concernant des pratiques RAL frauduleuses ou trompeuses ?

7. SÉCURITÉ

7.1. Des mesures de sécurité sont-elles prises pour protéger la confidentialité et l'intégrité des informations personnelles détenues par le service de RAL ? Si oui, lesquelles (mot de passe/ chiffrement/authentification, par exemple) ?

7.2. Des mesures de sécurité sont-elles prises pour protéger la confidentialité et l'intégrité des communications pendant la procédure ? Si oui, lesquelles (mot de passe/chiffrement/ authentification) ?

8. RÉSULTAT DU RAL

8.1. L'issue de la procédure est-elle notifiée aux tiers ?

8.2. Si les parties n'exécutent pas de leur plein gré la décision rendue dans le cadre du RAL, celui-ci dispose-t-il d'un quelconque moyen de la faire appliquer (dépôt d'une caution, politique de remboursement, interdiction d'utilisation d'un sceau, etc.) ?

8.3. Si une partie conteste l'issue de la procédure :

Les motifs de cette contestation sont-ils prévus par le RAL ?
Le droit applicable est-il défini à l'avance ?
La juridiction compétente est-elle définie à l'avance ?

9. DÉSACCORDS AVEC LE SERVICE DE RAL

9.1. Le service de RAL limite-t-il sa responsabilité juridique ?

9.2. Si une partie conteste cette responsabilité :

Le droit applicable est-il défini à l'avance ?
La juridiction compétente est-elle définie à l'avance ?

1. A l'OCDE, l'organisation de la conférence est assurée par le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) du Comité PIIC et le Comité de la politique à l'égard des consommateurs (CPC) en coopération avec le Comité consultatif économique et industriel auprès de l'OCDE (BIAC).

2. « ADR That Works » d'Ernest G. Tannis - la citation est reprise du manuel de règlement alternatif des litiges de l'American Bar Association (Appendix E).

3. Dans la plupart des cas, l'une des parties dépose une réclamation auprès d'un tiers prestataire de règlement alternatif qui notifie la réclamation à l'autre partie ou aux autres. Ensuite, un échange ou une série d'échanges ont lieu entre les parties en présence du tiers neutre alors que les parties tentent de régler le litige. Ce tiers neutre peut être un médiateur ou un arbitre humain ou un système automatique comme dans le cas de logiciels informatiques qui règlent les litiges de police d'assurance. Les parties peuvent convenir des règles de la procédure ou le prestataire de règlement alternatif peut les imposer : l'issue définitive du processus de règlement peut être un accord trouvé par les parties elles-mêmes ou un jugement imposé par un tiers : l'issue peut être non contraignante pour les deux parties, contraignante pour l'une d'elles seulement ou pour les deux parties à la fois.

4. La négociation assistée (ou conciliation) est un processus informel par lequel un tiers neutre oriente les parties vers un compromis.

5. L'arbitrage est un processus par lequel les parties soumettent les faits de leur litige et leurs arguments (de vive voix ou par écrit) à un ou plusieurs décideurs indépendants qui statuent sur l'affaire en respectant l'équité ou la loi. L'arbitrage est juridiquement contraignant et le plus souvent définitif.

6. Cf. Appendice A.

7. www.oecd.org/dataoecd/39/13/1840065.pdf.

8. DSTI/CP(98)12/FINAL

9 . *Guidelines for Consumer Protection in the Context of Electronic Commerce,* approuvée le 9 décembre 1999 par le Conseil de l'OCDE, disponible à: www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

10. DSTI/ICCP/REG/(99)15 FINAL, déclassé le 15 septembre 2000, disponible à www.olis.oecd.org/olis/1999doc.nsf/LinkTo/dsti-iccp-reg(99)15-final.

11. Documents relatifs disponibles à www3.ftc.gov/os/2000/02/altdisputeresolutionfrn.htm.

12. Disponible à www.ita.doc.gov/td/industry/otea/ecommerce/apec/.

13. Informations disponibles à www.gbde.org/acrobat/miami00.pdf.

14. 123Settle.com, par exemple, permet aux parties au départ de signer un accord pour s'en tenir à l'issue trouvée automatiquement ou pour visionner d'abord leur hypothèse de règlement (si un règlement est possible), puis de décider de signer ou non un engagement de respect du règlement. Un autre système au moins, en cours de développement, OnlineDisputes.org, ne prévoit pas que les parties soient engagées par l'issue trouvée : par ailleurs, il permet aux parties de régler d'autres litiges que ceux liés au paiement au comptant, comme les échanges de produits entre consommateurs.

15 . EBay renvoie à des clients ayant des litiges avec SquareTrade via son site Internet.

16. Albert Benshop, Peculiarities of Cyberspace « Building Blocks for an Internet Sociology »

17. Albert Benshop, *ibid*.

18. Par exemple, les Lignes directrices de l'OCDE régissant la protection de la vie privée, les Lignes directrices de l'OCDE régissant la protection des consommateurs ou tout autre ensemble de règles ou de principes directeurs internationaux.

19. Les parties ou le tribunal d'arbitrage peuvent s'adresser à un juge d'appui en cas de difficultés dans l'organisation, la mise en œuvre et l'application de la procédure d'arbitrage. Ce juge n'est pas là pour contester la procédure, mais pour apporter son aide à la procédure d'arbitrage. On peut lui demander d'intervenir dans la constitution du tribunal d'arbitrage (soit d'emblée soit au cours de la procédure d'arbitrage, si le tribunal est tronqué et les parties ou arbitres restants ne parviennent pas à un accord pour rectifier la situation). Il peut également être sollicité, notamment dans des cas d'urgence (même si le droit national ne reconnaît pas toujours ce rôle), en cas de difficulté à obtenir des preuves (plus

rarement) et pour faire exécuter les mesures ordonnées par le tribunal d'arbitrage. Son rôle exact dépend du droit applicable à l'arbitrage, qui peut être différent du droit applicable à la cause du différend et du droit applicable à la procédure d'arbitrage elle-même.

20. La signature électronique désigne toute action exprimant l'intention de signer (convenir de quelque chose ou accepter), telle que l'indication d'un nom à la fin d'un courrier électronique, un clic sur le bouton « J'accepte » à l'écran ou l'utilisation de la signature électronique d'une instance de certification. Lorsqu'une signature électronique est certifiée, par quelque méthode que ce soit, afin de garantir l'identité et/ou l'authenticité du document signé, elle devient une authentification électronique. En d'autres termes, on peut dire que l'authentification électronique englobe toute méthode de vérification d'une information dans un environnement électronique, qu'il s'agisse de l'identité de l'auteur d'un texte ou de l'émetteur d'un message, l'autorisation donnée à une personne de participer à un certain type de transaction, les dispositifs de sécurité des matériels et des logiciels ou l'une quelconque des innombrables autres informations qu'un individu souhaite pouvoir confirmer dans un environnement électronique.

Chapitre 9

DISPOSITIONS JURIDIQUES LIÉES AU RÈGLEMENT ALTERNATIF DES LITIGES ENTRE ENTREPRISES ET CONSOMMATEURS RELATIFS À LA VIE PRIVÉE ET À LA PROTECTION DES CONSOMMATEURS

L'objet de ce document est d'examiner l'incidence des dispositions juridiques nationales actuelles sur le recours au règlement alternatif des litiges (RAL) dans le cadre du commerce électronique. Il y est présenté une synthèse des réponses des pays membres au Questionnaire sur les dispositions juridiques liées au règlement alternatif des litiges (RAL) entre entreprises et consommateurs relatifs à la vie privée et à la protection des consommateurs (joint en annexe), et comporte un résumé des principaux points, une introduction, une synthèse des réponses reçues et quelques commentaires en conclusion.

Chapitre 9

DISPOSITIONS JURIDIQUES LIÉES AU RÈGLEMENT ALTERNATIF DES LITIGES ENTRE ENTREPRISES ET CONSOMMATEURS RELATIFS À LA VIE PRIVÉE ET À LA PROTECTION DES CONSOMMATEURS

Principaux points

Les nombreux instruments nationaux liés au règlement alternatif des litiges (RAL) qui ont été signalés par les pays membres ne sont pas spécifiques à l'environnement en ligne[1], mais en faire l'inventaire contribue à fournir une vue générale de la nature et de l'étendue de l'application des dispositions actuelles relatives au RAL dans la plupart de ces pays et pourrait servir de base pour des travaux ultérieurs visant à faciliter le RAL pour les litiges en ligne au niveau transfrontière.

Les pays membres reconnaissent les avantages potentiels du RAL informel et l'encouragent.

L'importance que les pays membres attachent au RAL informel est l'un des thèmes communs aux réponses au questionnaire. La plupart des pays ont pris des initiatives reconnaissant les avantages potentiels du RAL. Ces initiatives visent à favoriser la création de mécanismes efficaces, adaptés et peu coûteux, pour remplacer le règlement formel des litiges devant les tribunaux[2].

Les dispositifs de RAL créés, financés ou gérés par l'État pour traiter les litiges traditionnels sont courants dans les pays membres.

Les dispositions juridiques créant des types particuliers de RAL pour les litiges traditionnels, tels que le RAL rattaché à un tribunal ou celui destiné aux litiges entre propriétaires et locataires, sont courantes dans les pays membres. Elles vont des médiateurs de la consommation aux commissions d'arbitrage, en passant par les tribunaux de conciliation. Les compétences de ces instances se limitent généralement soit à un type particulier de litige, soit à un secteur spécifique. Le recours à ces dispositifs est obligatoire ou encouragé.

Il y a peu de réglementations générales relatives au RAL dans les pays membres : l'image la plus fréquente est celle d'un patchwork de textes.

Les pays membres ne possèdent pas de structure-cadre de réglementation du RAL formel ou informel. Dans bon nombre d'entre eux, l'arbitrage est réglementé, mais les types informels de RAL ne le sont en général pas. Beaucoup de pays possèdent cependant des dispositions s'appliquant aux litiges entre entreprises et consommateurs dans des contextes spécifiques. Des règles ont été établies pour différents types de RAL, selon l'objet du litige (protection de la vie privée, par exemple), la transaction concernée (assurance, télécommunications), l'importance, le montant et la complexité du litige, le recours à l'arbitrage ou à la médiation, etc.

Dans la plupart des pays membres, les parties sont généralement libres d'accepter un RAL non contraignant dans un cadre contractuel.

Le recours au RAL entre entreprises et consommateurs informel ne fait pas l'objet de restrictions juridiques spéciales. Dans la plupart des pays, les parties sont libres d'accepter le RAL dans un cadre contractuel, sous réserve des restrictions s'appliquant généralement aux contrats, tels que le dol, la contrainte ou l'ordre public (impossibilité de renoncer à certains droits, clauses exorbitantes ou léonines et questions d'équité et de loyauté, par exemple). Ces considérations semblent représenter une limite d'ordre général au recours au RAL obligatoire ou contraignant et à sa mise en œuvre.

Introduction

Afin de mieux comprendre le rôle que peut jouer le RAL pour renforcer la confiance des utilisateurs et des consommateurs dans le commerce électronique, l'OCDE, la Chambre de Commerce Internationale et la Conférence de droit international privé de La Haye ont organisé conjointement une conférence sur le RAL pour les litiges en ligne liés à la vie privée et à la protection des consommateurs. Elle s'est tenue à La Haye en décembre 2000 et a exploré l'utilisation des systèmes de RAL pour les litiges en ligne entre les entreprises et les consommateurs portant sur un faible montant et/ou impliquant un faible préjudice. Cette conférence s'est particulièrement intéressée aux systèmes informels souples qui permettent d'assurer l'équilibre requis entre le type de litige et le formalisme du processus de règlement.

Lors de leurs réunions de février et mars 2001, le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) et le Comité sur la politique à l'égard des consommateurs (CPC) ont décidé, dans le prolongement de la Conférence de la Haye, de poursuivre leurs travaux pour mieux sensibiliser les utilisateurs et les consommateurs au RAL pour les litiges en ligne et encourager le recours à un RAL entre entreprises et consommateurs juste et efficace pour ce type de litiges. Leur initiative se composait de trois volets : une mise à jour de l'inventaire des mécanismes de RAL pour les litiges en ligne, un instrument d'information pour les parties susceptibles d'avoir recours au RAL en ligne et un questionnaire sur les aspects juridiques.

Le questionnaire sur les aspects juridiques (voir l'annexe) a été établi par le Secrétariat, aidé de délégués du GTSIVP et du CPC, qui ont participé au projet par le biais d'un groupe de discussion électronique. En juin 2001, le questionnaire a été adressé aux pays membres et aux autres acteurs.

Le Secrétariat a reçu des réponses au questionnaire de 24 pays membres : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Hongrie, l'Italie, le Japon, le Mexique, la Nouvelle-Zélande, les Pays-Bas, la Pologne, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse et la Turquie. Il a également reçu des réponses du Centre de recherche informatique et droit (CRID) de l'université de Namur, en Belgique, du *Confcommercio* (Fédération du commerce de détail italien) et de deux prestataires en ligne de services de RAL, TRUSTe et SquareTrade.

L'objectif du questionnaire consistait à permettre d'acquérir une vue d'ensemble des régimes juridiques nationaux applicables au RAL entre entreprises et consommateurs dans les pays membres et à comprendre le rôle et l'incidence des dispositions juridiques en vigueur sur le recours au RAL, en particulier dans le cadre de l'environnement en ligne. Les questions visaient à obtenir des informations factuelles sur le contenu des dispositions juridiques (générales et spécifiques) applicables au RAL, dans un contexte national ou transfrontière.

Les conclusions pouvant être tirées des réponses au questionnaire sont limitées par plusieurs facteurs. Tout d'abord, il était difficile de répondre au large éventail de questions de manière absolue. Pour les pays dotés d'un système juridique dans lequel les compétences en matière de RAL sont partagées par les

autorités nationales et régionales ou locales, il n'a pas toujours été possible de décrire toutes les réglementations pertinentes. De même, le fait que les dispositions juridiques relatives au RAL ne soient généralement pas regroupées dans un seul ensemble de règles n'a pas facilité l'obtention de réponses complètes. Enfin, les comparaisons entre les pays ont été rendues difficiles par les différences existant entre les définitions nationales des mécanismes de RAL (médiation ou arbitrage par exemple).

Malgré ces limitations, un certain nombre de points communs ressortent des réponses fournies par les pays membres.

Dispositions générales relatives au RAL

Certains pays membres possèdent des dispositions spécifiques obligeant ou incitant les parties à recourir au RAL informel pour certains types de litiges. Outre les dispositions législatives et réglementaires, la majorité des pays ont fait référence, dans leur réponse, à des politiques générales d'encouragement des consommateurs à recourir au RAL informel, notamment lorsque des dispositifs publics ont été mis en place. D'autres pays possèdent des dispositions spécifiques interdisant ou limitant le recours au RAL dans certaines circonstances.

Dispositions encourageant ou imposant le RAL

L'Australie, le Canada, les États-Unis, l'Italie, le Japon, la Nouvelle-Zélande et le Royaume-Uni possèdent des dispositions encourageant le recours au RAL pour certains litiges. Au Royaume-Uni, des protocoles concernant la phase préparatoire du procès dans les cas de diffamation, de dommages corporels, de litige médical, de faute professionnelle et de questions liées à la construction et à l'ingénierie encouragent le recours au RAL. En Australie, le *Fair Trading Tribunal Act* de 1998 encourage expressément l'utilisation du RAL pour la résolution des litiges portés devant les tribunaux.

L'Allemagne, l'Autriche, le Canada, les États-Unis, la France, l'Italie, le Japon, la Nouvelle-Zélande et le Royaume-Uni possèdent des dispositions qui, dans certains cas, exigent explicitement des parties qu'elles épuisent toutes les possibilités de RAL avant toute action judiciaire.

Dispositions imposant le RAL avant de saisir les tribunaux

Certains pays exigent des parties, dans des cas précis, qu'elles épuisent toutes les possibilités de RAL avant de saisir un tribunal. Ainsi, l'Allemagne possède une législation régionale rendant la conciliation obligatoire dans le cas de litiges relatifs au droit des biens, aux petites créances, au droit de voisinage et aux actions pour atteinte à la réputation. En Autriche et en Suisse, les litiges entre propriétaires et locataires doivent être portés devant un organe public de RAL spécifique. En France, si aucun accord sur le montant du loyer ne peut être obtenu au moment du renouvellement du bail de location, les parties doivent saisir la Commission départementale de conciliation avant d'agir en justice[3].

Dispositions imposant le RAL après saisine d'un tribunal (dispositifs rattachés aux tribunaux)

Certains pays possèdent une législation permettant aux tribunaux d'exiger des parties qui les ont saisis d'avoir recours au RAL dans des circonstances précises et pour des affaires relevant de leur compétence. Les pays ayant signalé ce type de dispositions sont l'Australie, le Canada, les États-Unis, l'Italie, le Japon et la Nouvelle-Zélande. Ainsi, en Australie, le *Tenancy Tribunal Act* de 1994 impose la médiation comme méthode préalable de résolution des litiges entre les parties voulant agir en justice. Au Canada, la législation nationale exige de toutes les parties à un litige de droit civil qu'elles

participent à une médiation après le dépôt des conclusions. En Colombie britannique, toujours au Canada, une réunion obligatoire de règlement conduite de manière informelle par un juge a lieu pour les litiges de faible montant.

Suivant la même tendance, les Pays-Bas ont indiqué avoir récemment lancé des projets de médiation rattachés aux tribunaux de manière expérimentale dans cinq tribunaux du pays. Ce dispositif permet aux juges d'exiger des parties qu'elles tentent de trouver une solution avec l'aide d'un médiateur pour des affaires de droit administratif et civil spécifiques (comme la médiation familiale par exemple). Aux États-Unis, consécutivement à toute une série de lois, certains tribunaux fédéraux et des états exigent des parties qu'elles épuisent d'abord toutes les possibilités de RAL après saisine du juge, avant que le procès puisse se poursuivre. Ainsi, dans la plupart des affaires de droit civil du Maine, après avoir saisi le tribunal, les parties doivent tenir une réunion de RAL pour tenter de résoudre le litige[4].

Dispositions interdisant ou limitant le recours au RAL

Certains pays possèdent des dispositions interdisant ou limitant le recours au RAL. L'Allemagne, la France et l'Italie ont fait savoir que les parties ne pouvaient généralement pas chercher à résoudre par le RAL les litiges impliquant des droits inaliénables ou non disposables (divorce, litiges familiaux, etc.). De même, le Mexique a cité des dispositions juridiques interdisant de résoudre certains litiges, tels que les conflits familiaux et le divorce, par l'arbitrage[5]. Aux États-Unis, les parties ne sont pas tenues d'utiliser le RAL rattaché aux tribunaux pour certains litiges, notamment ceux concernant les droits constitutionnels[6]. Elles peuvent néanmoins décider de leur plein gré de tenter de les résoudre par le bais d'un RAL privé.

L'Allemagne, la Corée, le Danemark, l'Espagne, la Finlande, les Pays-Bas, la Pologne, la Suède et la Suisse ont mis en place des dispositifs nationaux de RAL qui ne peuvent pas s'appliquer à certains types d'affaires (supérieures à un montant déterminé, par exemple) ou à certaines parties (exclusion des litiges entre les entreprises et l'administration, entre autres). Aux Pays-Bas, les commissions agréées chargées des plaintes ne sont pas compétentes pour régler certains litiges, comme ceux liés au décès, aux dommages corporels ou à la maladie. En Suisse, dans le cadre du Concordat (accord d'arbitrage), les parties ne sont pas libres d'utiliser l'arbitrage si l'affaire relève de la compétence exclusive d'une autorité publique.

Épuisement de toutes les possibilités de RAL

Peu de pays membres signalent des dispositions spéciales affectant éventuellement la validité des dispositions contractuelles visant à épuiser toutes les possibilités de recours au RAL avant de chercher réparation auprès des tribunaux.

La Corée, l'Espagne, les États-Unis et la Nouvelle-Zélande ont indiqué que les dispositions contractuelles visant à épuiser toutes les possibilités de RAL seraient probablement exécutoires. Ainsi, aux États-Unis, de telles dispositions sont généralement valides, à moins que les parties demandant leur annulation puissent prouver qu'elles ont été obtenues par dol, contrainte, erreur, abus ou illégalement. L'Australie, le Canada et le Japon ont indiqué que les parties pouvaient conclure un contrat prévoyant l'épuisement de toutes les possibilités de RAL. Ils ont cependant souligné que ces dispositions pouvaient être écartées ou annulées par les tribunaux pour « clause contractuelle abusive » ou pour toute autre irrégularité, telle qu'influence abusive, violation de l'ordre public ou restriction de l'accès des consommateurs aux voies de recours ordinaires.

La plupart des pays de l'Union européenne ont fait référence à la directive européenne concernant les clauses abusives dans les contrats, qui ne permet pas, en soi, aux consommateurs de renoncer à leur droit de saisir un tribunal. Ils ont également mentionné les lois nationales de mise en œuvre [de la directive] comme autre fondement d'une éventuelle annulation d'un contrat s'il a pour effet de restreindre l'accès aux voies de recours ordinaires. Ainsi, l'Autriche a cité des dispositions de sa loi relative à la protection des consommateurs, qui déclarent nuls les contrats privant les consommateurs de leur droit de saisir un tribunal. De même, le Code civil italien dispose que toute clause de contrat entre entreprises et consommateurs concernant ou entraînant des exceptions à la compétence des tribunaux est présumée abusive. Les autres pays citant dans ce contexte leur législation nationale relative aux clauses contractuelles abusives ou la directive européenne sont le Danemark, la Finlande, la France, l'Italie, les Pays-Bas, le Royaume-Uni et la Suède. Dans un cadre plus large, le Mexique a fait observer que sa loi fédérale relative à la protection des consommateurs invalide également les clauses « contraire aux droits des consommateurs » d'une manière générale.

RAL contraignant

Il n'existe généralement aucune disposition spécifique interdisant aux parties à un contrat d'être liées par le RAL après la naissance d'un litige, ni, *a fortiori,* à l'issue d'une procédure de RAL. Ainsi, l'Autriche, la France et l'Italie ont relevé que, dans le cas d'un accord signé à l'issue d'une procédure de RAL, l'autonomie contractuelle est reconnue et les accords signés par les parties seront contraignants conformément au droit des contrats.

Cependant, il apparaît généralement que les dispositions contractuelles obligeant les parties à recourir à un RAL avant la naissance d'un litige peuvent être considérées comme « abusives » ou contraires à l'ordre public, notamment si elles privent les consommateurs de leur droit de saisir un tribunal. Les pays ayant adopté cette approche sont l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, la Finlande, la France, l'Italie, le Japon, les Pays-Bas et la Suède. Les législations suédoise et française, par exemple, stipulent que les contrats de consommation conclus avant un litige et contenant une clause d'arbitrage sont automatiquement invalides pour clause abusive. De même, au Royaume-Uni, un accord d'arbitrage est automatiquement considéré comme abusif à l'égard du consommateur, en particulier s'il concerne une créance de faible montant.

Les États-Unis et la Nouvelle-Zélande ont fait observer que, dans la pratique, les consommateurs sont libres d'accepter d'être liés par le RAL, mais que c'est le droit des contrats qui déterminera en fin de compte la validité d'un contrat visant à accepter le RAL et à s'y soumettre. Ainsi, aux États-Unis, les contrats ne sont pas nuls simplement parce qu'ils privent les consommateurs de leur droit de saisir un tribunal – la validité du contrat est alors jugée au cas par cas. La règle générale est que ce type de contrat est valide, irrévocable et exécutoire, sauf s'il contrevient aux principes généraux du droit des contrats, relatifs notamment au dol, à la contrainte ou à l'abus. La législation japonaise stipule également qu'un accord visant à soumettre les litiges futurs à l'arbitrage est valable tant qu'il concerne des rapports de droit déterminés et les litiges en découlant.

Mise en œuvre et exécution judiciaire des résultats du RAL

Bon nombre de résultats du RAL sont mis en œuvre par consentement des parties et ne nécessitent donc pas l'intervention de tiers. Cependant, lorsque l'une de parties refuse de se soumettre à un accord de RAL, de nombreux pays ont indiqué qu'ils possédaient des mécanismes d'exécution d'un tel accord. Dans la cadre transfrontière (litiges entre entreprises et consommateurs), les modalités d'exécution des décisions issues du RAL impliquant des parties de différents pays demeurent floues.

Les États-Unis, le Japon, la Nouvelle-Zélande et le Royaume-Uni ont indiqué que les décisions issues d'un RAL de type médiation ou conciliation pouvaient être exécutées en justice dans le cadre des grands principes du droit des contrats. D'autres pays possèdent des dispositions législatives spécifiques prévoyant des mécanismes d'exécution des décisions issues du RAL au niveau national. Ainsi, aux Pays-Bas, les accords conclus après une procédure de médiation peuvent généralement être soumis au tribunal afin d'être confirmés par un juge. En France, en cas de conciliation extrajudiciaire, le tribunal peut donner force exécutoire à l'accord entre les parties, avec leur consentement[7].

Certains pays ont également indiqué que les accords de RAL conclus au cours du procès (dans le cadre du RAL rattaché aux tribunaux, par exemple) peuvent obtenir le statut de jugement sur demande au tribunal, avec le consentement des deux parties. L'Australie, les États-Unis, la France, le Japon et le Royaume-Uni ont fait état d'une telle approche. En France, les tribunaux jouent ainsi un rôle général de conciliation qui implique que, si les parties parviennent à un accord au cours de la procédure, elles peuvent à tout moment demander au tribunal de valider cet accord ou le tribunal peut de son propre chef préparer un accord de conciliation que les parties pourront signer. De la même manière, le Canada a fait savoir que les décisions issues du RAL pouvaient être exécutées avec le consentement des parties, auquel cas l'accord de RAL forme le fondement d'une décision d'accord amiable ayant le même statut que tout autre jugement rendu par un tribunal.

L'Allemagne, l'Autriche, la Corée, l'Espagne, la Hongrie, l'Italie, le Mexique, la Pologne, la Suisse et la Turquie ont indiqué que les décisions de RAL rendues par des organes opérant dans le cadre de dispositifs nationaux pouvaient être exécutées dans certains cas. Ainsi, la loi fédérale mexicaine relative à la protection des consommateurs stipule que les décisions rendues ou les accords approuvés par le PROFECO (Bureau du procureur chargé de la protection des consommateurs) dans le cadre de ses procédures de conciliation ou d'arbitrage constituent par nature des jugements définitifs et doivent être mis en œuvre par les parties ou exécutés par les tribunaux. En Autriche, toute décision adoptée par l'organe approprié de RAL relativement à la législation sur les baux locatifs constitue un « titre exécutoire » et est donc exécutoire comme tel, sous réserve que le litige ne soit pas porté devant un tribunal dans les quatre semaines suivant la notification de la décision du RAL. Le Danemark et la Finlande ont en revanche fait savoir que les décisions ou les recommandations des Commissions chargées des plaintes des consommateurs n'étaient ni exécutoires ni contraignantes.

Enfin, quelques pays ont mentionné des limites législatives spécifiques à la mise en œuvre des décisions issues du RAL rendues par des organes officiels particuliers ou dans le cadre d'un arbitrage. Ainsi, la loi japonaise relative aux procédures d'assignation et d'arbitrage stipule que chaque partie peut demander l'annulation d'une décision dans certains cas déterminés, y compris par exemple si la décision exige d'une partie qu'elle commette un acte interdit par la loi. La législation du Royaume-Uni relative à l'arbitrage stipule quant à elle qu'un accord d'arbitrage peut être « écarté » si le tribunal considère que cet accord est « nul et non avenu », inapplicable ou impossible à honorer. Aux Pays-Bas, lorsque la décision issue d'une procédure d'arbitrage ou d'avis contraignant est manifestement contraire à la morale publique ou à l'ordre public, sa mise en œuvre en sera affectée[8]. Il existe d'autres dispositions législatives spécifiques aux États-Unis, en France, au Mexique, en Pologne, en République tchèque, en Suisse et en Turquie.

Garanties procédurales du RAL

Dans certains pays membres, des dispositions législatives imposent des garanties procédurales applicables à un vaste éventail de dispositifs de RAL. D'autres pays ne possèdent de garanties procédurales que pour un type particulier de RAL ou pour le RAL portant sur un type particulier de litige.

Confidentialité

Les États-Unis ont mentionné l'existence d'une législation spécifique relative à la confidentialité des actes ou résultats intervenant dans le cadre du RAL. Ils ont ajouté que certaines législations d'État garantissaient la confidentialité. Ainsi, dans l'Ohio, la loi sur la confidentialité de la médiation impose que toute communication liée à la médiation soit confidentielle, à quelques exceptions près[9].

Les règles de confidentialité des dispositifs de RAL gérés par l'État sont variables. En Suède, l'organe de RAL actuel est une autorité publique. Toutes les procédures sont donc généralement publiques, mais une décision peut être confidentielle si elle contient des informations personnelles ou professionnelles sensibles. Une approche similaire est suivie en Pologne, où les procès du Tribunal de conciliation sont publics, sauf si cela va à l'encontre de l'ordre public ou s'ils risquent de révéler des secrets d'État ou commerciaux. De même, en Corée, au Danemark et en Finlande, la législation visant à assurer l'accès du public aux procédures publiques s'applique aux organes de RAL gérés par l'État et prévaut sur tout accord en matière de confidentialité. Ainsi, au Danemark, la législation relative à la publicité des actes de l'administration s'applique de telle manière que les informations relatives aux procédures ou aux décisions issues d'un RAL peuvent être divulguées à une tierce personne à sa demande.

En Suisse en revanche, les procédures d'arbitrage des organes publics sont généralement confidentielles, mais si l'une des parties fait appel d'une décision, l'instance d'appel a accès à l'ensemble des informations relatives à la procédure de RAL.

L'Australie, la France et le Japon ont mentionné l'existence de garanties applicables au RAL dans le cadre judiciaire (ou au RAL rattaché aux tribunaux). En France, par exemple, des garanties ont été introduites dans les procédures de conciliation conduites par les conciliateurs de justice et les procédures de médiation conduites par les médiateurs désignés par un tribunal. Elles garantissent notamment la confidentialité des procédures. Au Japon, les affaires de conciliation sont confidentielles, conformément à la loi relative à la conciliation en matière civile, mais les parties et les personnes concernées peuvent demander à consulter le dossier de l'affaire ou en prendre copie, sauf si cela porte atteinte au déroulement du dossier ou aux fonctions du tribunal. Dans certains pays, la loi considère même les informations provenant d'une procédure de RAL comme des preuves irrecevables. En Australie, le *Federal Court Act* stipule que tout ce qui a été dit ou déclaré au cours d'une médiation rattachée à un tribunal constitue une preuve irrecevable par tout tribunal et dans toute action en justice.

Plusieurs membres ont néanmoins indiqué que, dans la pratique, les parties peuvent être obligées dans certains cas de divulguer des informations relatives à une procédure de RAL, qu'elles soient convenues ou non de garder la procédure confidentielle. L'Australie, le Canada, la France, l'Italie, le Mexique, la Nouvelle-Zélande[10], les Pays-Bas, le Royaume-Uni et la Suisse ont souligné cette approche. Le Mexique, par exemple, a fait observer que la loi fédérale de protection des consommateurs stipule que les autorités, les prestataires d'un service de RAL et les consommateurs doivent fournir au PROFECO, le procureur chargé de la protection des consommateurs, toute information nécessaire à l'instruction. L'Australie et le Canada ont quant à eux précisé que les professionnels du RAL (médiateurs, etc.) sont, d'un point de vue déontologique, tenus de divulguer certaines informations si cela est nécessaire à la prévention d'un préjudice grave. Ils ont ajouté que les tribunaux semblaient d'une manière générale disposer d'un pouvoir discrétionnaire dans ce cas : ils peuvent en effet respecter la confidentialité au nom de l'intérêt public, mais ils peuvent également décider que les considérations d'intérêt public prévalent sur l'accord de confidentialité.

Aptitude et impartialité des prestataires d'un RAL

La plupart des pays membres ont signalé l'existence de dispositions réglementant spécifiquement l'aptitude et l'impartialité des professionnels dans le RAL rattaché ou soumis aux tribunaux. Les pays ayant cité ce type de réglementation sont l'Australie, le Canada, les États-Unis, la France, le Japon et les Pays-Bas. En France, le Code de procédure civile impose certaines obligations aux conciliateurs et aux médiateurs de justice. Les conciliateurs doivent par exemple avoir trois ans d'expérience dans le domaine du droit, mais il n'existe aucune condition générale obligatoire pour les services extrajudiciaires. Aux États-Unis, certains tribunaux ou parlements des états imposent des critères de formation ou d'expérience aux médiateurs travaillant dans les dispositifs de médiation de l'état ou financés par les tribunaux.

L'Allemagne, l'Autriche, la Corée, le Danemark, l'Espagne, la Finlande, la Hongrie, l'Italie, le Japon, le Mexique, la Pologne, la République slovaque, le Royaume-Uni, la Suède et la Suisse ont cité des dispositions réglementant les qualifications et l'impartialité des professionnels du RAL dans les organes créés par la loi. Par exemple, la législation danoise établissant la Commission chargée des plaintes des consommateurs comporte des dispositions qui détaillent la composition de cette instance (et donc les personnes pouvant jouer le rôle d'intermédiaire).

Certains pays membres imposent également des règles d'aptitude et d'impartialité dans le cas des services généraux de RAL. L'Australie a fait référence à sa législation des états ou des territoires relative à l'accréditation des médiateurs. Au Japon, les ministres compétents certifient les organisations ayant pour objet de régler les litiges relatifs à la vie privée et aux informations personnelles. Les personnes se consacrant au RAL de manière lucrative doivent en principe pouvoir justifier d'une formation de juriste. Aux États-Unis, la profession de prestataire de services de RAL est très peu réglementée. Dans la plupart des états, une personne peut offrir des services privés de médiation sans formation, examen, autorisation ou accréditation spéciale. Dans la pratique, la plupart des dispositifs indépendants de médiation et des organisations de professionnels de la médiation imposent cependant aux médiateurs leurs propres normes de formation ou d'expérience[11]. Enfin, la Nouvelle-Zélande a fait savoir que les avocats proposaient généralement des services de RAL et étaient soumis à ce titre à des critères déontologiques et à des procédures disciplinaires. Le Mexique et la République tchèque ont également mentionné des dispositions s'appliquant dans le cadre de l'arbitrage. La loi fédérale mexicaine de protection des consommateurs réglemente par exemple l'agrément des arbitres indépendants des litiges liés à la consommation.

Autres garanties procédurales

Au Canada (uniquement pour les litiges entre entreprises), aux États-Unis, au Japon et au Mexique (uniquement pour les litiges entre entreprises pour ces deux derniers pays), en Nouvelle-Zélande, aux Pays-Bas, en République tchèque (uniquement pour les litiges entre entreprises) et au Royaume-Uni, certaines garanties procédurales s'appliquent à l'arbitrage. En Nouvelle-Zélande par exemple, l'*Arbitration Act* de 1996 contient certaines obligations procédurales et stipule qu'un accord peut être écarté si la partie requérante n'a pas dûment reçu notification de la nomination d'un arbitre ou de la procédure d'arbitrage, ou si elle était de toute autre manière dans l'impossibilité de faire valoir son point de vue.

L'Australie, l'Autriche, la Corée, le Danemark, l'Espagne, la Finlande, l'Italie, le Mexique, les Pays-Bas, la Pologne, la Suède et la Suisse ont indiqué que les autorités et organes publics conduisant des dispositifs de RAL au niveau national ou d'un état/territoire devaient offrir certaines garanties. En Corée par exemple, la loi définit les garanties procédurales s'appliquant aux procédures de RAL conduites par la Commission de règlement des litiges liés à la consommation, telles que la

composition de la commission, la durée du mandat de ses membres, les quorums de décision et les délais de prise de décision.

Du point de vue de la réglementation générale des procédures de RAL, les États-Unis ont cité des dispositions spécifiques régissant les procédures applicables aux litiges entre entreprises et consommateurs concernant les questions de garantie. Le *Magnuson Moss Warranty Act* exige de la Commission fédérale du commerce des États-Unis qu'elle fixe des obligations minimales pour les procédures de règlement des litiges. Ainsi, tout mécanisme de règlement d'un litige lié à la consommation régi par cette loi doit, entre autres, être en mesure de régler les litiges de manière indépendante, sans être influencé par les parties en présence, suivre des procédures écrites et offrir à chacune des parties la possibilité d'exposer son point de vue, de l'étayer de preuves et de réfuter le point de vue exprimé par la partie adverse. Il existe également au niveau des états des réglementations conférant le droit de représentation dans les négociations de médiation. Ainsi, en Alaska et dans le Dakota du Nord, la loi interdit aux médiateurs d'exclure un avocat des réunions de médiation.

Outre la loi, on peut observer d'autres initiatives de réglementation visant à introduire des garanties dans le RAL. La recommandation de la Commission européenne concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation, et les critères pour la résolution des litiges commerciaux (initiative de réglementation commune) en Australie, ont été cités à ce propos.

La Nouvelle-Zélande et le Royaume-Uni ont également indiqué que certaines garanties procédurales pouvaient être introduites « de fait » dans les procédures de RAL, puisque les médiateurs, les conciliateurs et les autres tiers impartiaux sont souvent tenus de se conformer à des codes déontologiques. En Nouvelle-Zélande par exemple, la plupart des RAL sont conduits par des avocats soumis à des obligations déontologiques et à des procédures disciplinaires, ce qui peut offrir certaines garanties procédurales, notamment du point de vue de l'indépendance, de l'impartialité et de la transparence.

Les États-Unis ont enfin mentionné l'existence de lignes directrices facultatives pour les prestataires de services de RAL chargés des litiges entre entreprises et consommateurs[12].

Le patchwork des mécanismes de RAL existants

Aucun des pays membres n'a signalé l'existence d'une structure-cadre de réglementation du RAL dans le cas des litiges entre entreprises et consommateurs. Un grand nombre de pays ont cependant fait référence à des dispositions s'appliquant aux litiges entre entreprises et consommateurs dans des contextes spécifiques. Des règles ont été établies pour différents types de RAL, selon l'objet du litige (la protection de la vie privée, par exemple), le type de transaction concernée (assurance, télécommunications), la dimension, le montant et la complexité du litige, le recours à l'arbitrage ou à la médiation, etc.

La plupart des pays offrent un dispositif créé, financé ou géré par l'État pour résoudre certains litiges de type entreprises-consommateurs. Ces dispositifs peuvent être classés en deux catégories : le RAL mixte public-privé et le RAL créé, financé ou géré par l'État.

RAL mixte public-privé

Certains pays ont créé des dispositifs de RAL résultant d'initiatives associant le secteur public et le secteur privé. La législation australienne peut par exemple rendre obligatoires les codes de conduite du secteur privé (qui comprennent souvent des dispositions relatives au RAL). Ainsi, le code de conduite pour la franchise sert de référence au Bureau du conseiller en médiation pour les litiges dans ce domaine. L'Australie s'est également dotée de dispositifs associant le secteur public et le secteur privé dans le domaine de la protection de la vie privée. Si un consommateur et une entreprise sont incapables de résoudre entre eux leurs litiges relatifs à la vie privée, le consommateur peut demander à une personne indépendante d'instruire le litige. Si l'entreprise concernée est soumise à un code sur la protection de la vie privée approuvé et comprenant un mécanisme d'examen des réclamations, la personne indépendante chargée de l'instruction sera l'arbitre désigné conformément au code. Dans le cas contraire, c'est le Commissaire fédéral à la protection de la vie privée qui prendra en charge l'affaire. En Autriche, dans le secteur des télécommunications, un organisme professionnel indépendant joue, entre autres, le rôle de bureau de conciliation et les prestataires de services de télécommunication doivent participer à la procédure.

La République slovaque a fait état d'une législation autorisant les associations non gouvernementales de consommateurs à arbitrer les litiges entre consommateurs et entreprises. Il existe deux groupements d'associations de consommateurs dans l'ensemble du pays, ainsi que plusieurs organisations régionales. La législation slovaque relative à la vente à distance et au démarchage à domicile autorise également les associations de consommateurs à arbitrer les litiges dans ce domaine.

RAL créé, financé ou géré par l'État

Organes chargés des plaintes d'ordre général des consommateurs

Pour traiter les plaintes des consommateurs, les pays membres ont créé divers organes prenant en charge d'une manière générale le RAL entre entreprises et consommateurs en cas de litiges entre les entreprises et les consommateurs. Le Danemark et la Finlande ont créé des commissions chargées des plaintes des consommateurs et l'Allemagne, l'Australie, la Corée, l'Espagne, la Hongrie, le Japon, le Mexique, la Nouvelle-Zélande, la Suède, la Suisse et la Turquie ont mis en œuvre divers autres mécanismes dans ce domaine. La Pologne a en outre mentionné un organe de RAL plus formel ou plus proche d'une instance judiciaire, appelé Tribunal de conciliation. Cet organe a été créé par la loi d'inspection du commerce et comporte une procédure formelle débutant par le dépôt d'une requête. Les parties se soumettent volontairement aux procédures de ce tribunal, mais une fois ces procédures et l'autorité du tribunal acceptées, les décisions de ce dernier sont aussi contraignantes que le jugement d'un tribunal ordinaire et il n'existe aucun droit d'appel. Par opposition à cette procédure formelle, les États-Unis ont déclaré qu'au niveau des états, un grand nombre de bureaux du procureur général ou d'agences de protection des consommateurs proposaient des dispositifs volontaires et informels de résolution des litiges de type entreprises-consommateurs.

Mécanismes de plainte pour certains secteurs d'activité ou types de litiges

Un certain nombre de pays membres ont également mis en œuvre des dispositifs ou des organes de RAL entre entreprises et consommateurs gérés par l'État, se consacrant uniquement aux plaintes des consommateurs dans une branche spécifique ou pour des types de litiges particuliers.

L'Allemagne, l'Australie, l'Autriche, le Canada, la Corée, l'Espagne, la Finlande, l'Italie, le Mexique, les Pays-Bas, la Suède et la Suisse ont mentionné de tels dispositifs gérés par l'État. Au

Mexique par exemple, la Commission nationale d'arbitrage médical a été créée pour arbitrer les litiges liés aux services médicaux. Le Mexique a également signalé l'existence d'une loi imposant le dépôt de plaintes dans le domaine des services financiers auprès de la Commission nationale de défense des usagers des services financiers[13]. Au Canada, la Commission des services financiers de l'Ontario a été créée pour résoudre par la médiation et l'arbitrage les litiges liés à l'assurance des véhicules à moteur. En Italie, la loi[14] prévoit la création de commissions d'arbitrage et de conciliation afin de résoudre les litiges entreprises-entreprises et entreprises-consommateurs relatifs aux services touristiques.

Le Canada, la Corée et la Nouvelle-Zélande ont mentionné des dispositifs gérés ou financés par l'État dans le domaine de la protection de la vie privée. En Corée, la loi[15] dispose que toute personne souhaitant la médiation d'un litige relatif à ses informations personnelles peut en effectuer la demande auprès de la Commission de médiation des litiges[16], qui instruit l'affaire et propose un projet de médiation aux parties dans un délai de 60 jours. Au Canada, des dispositions légales stipulent que le Commissaire à la protection de la vie privée peut inciter les plaignants à essayer de régler les litiges relatifs à la protection de la vie privée directement avec l'entreprise concernée ou instruire lui-même l'affaire. Il peut adresser des recommandations à une entreprise, rendre publique toute information sur les pratiques d'une société relatives à la protection de la vie privée ou renvoyer une plainte devant la Cour fédérale du Canada. En Nouvelle-Zélande, la loi[17] exige du Commissaire à la protection de la vie privée[18] qu'il s'efforce de parvenir à un accord. La méthode de RAL n'est pas précisée. Dans la pratique, le Commissaire règle généralement les plaintes par la négociation assistée, parallèlement à une procédure d'instruction. Il a recours à la médiation, le cas échéant.

L'Australie, l'Autriche, la France, les Pays-Bas et la Suède ont en outre mentionné des obligations spécifiques pour les litiges entre propriétaires et locataires. Aux Pays-Bas, la loi relative à la location de logements publics offre aux locataires la possibilité de saisir l'une des Commissions chargées des plaintes des locataires. Si aucune des parties n'a recours au tribunal pour la même affaire dans les deux mois, elles sont censées être parvenues à l'accord entériné par la décision de la Commission.

RAL rattaché aux tribunaux

En ce qui concerne le RAL rattaché ou soumis à un tribunal, l'Allemagne, l'Australie, le Canada, les États-Unis, la France, l'Italie, le Japon et le Royaume-Uni ont mentionné des dispositifs permettant aux tribunaux de renvoyer les litiges à une structure de RAL. Par exemple, la France a fait état d'un dispositif prévoyant la conciliation judiciaire, qui permet à un juge de désigner un conciliateur pour qu'il prête son concours au règlement à l'amiable du litige, avec l'accord des parties. Le conciliateur doit entendre le point de vue des parties et informer le juge des résultats de la procédure une fois celle-ci achevée. En cas d'accord amiable, celui-ci est soumis au juge pour approbation formelle. Dans le cas contraire, l'instance se poursuit devant le tribunal.

Réglementation du RAL hors du cadre entreprises-consommateurs

Bien que ce ne soit pas l'objet principal de cette étude, certains pays membres ont brièvement décrit leur réglementation en dehors du cadre des litiges entre entreprises et consommateurs et mentionné des dispositions spécifiques s'appliquant au RAL pour les litiges entre entreprises, de consommateur à consommateur, d'entreprise à administration et de consommateur à administration.

L'Australie, la Corée, la France, l'Italie et la Suisse ont notamment mentionné des dispositifs de RAL gérés par l'État pour les litiges impliquant ce dernier. Ainsi, en Australie, des dispositions[19] prévoient des réunions (conciliation) et une médiation pour les décisions administratives du Commonwealth concernant les entreprises ou les consommateurs, pour les questions administratives

(les questions fiscales, par exemple) ou pour la conciliation en cas de plainte des consommateurs à l'encontre d'organismes publics (accès des handicapés aux bâtiments publics, discrimination raciale, etc.). Certains cantons suisses ont créé des systèmes de médiateurs pour résoudre les litiges entre les consommateurs et l'administration et ceux entre les salariés du secteur public et leurs supérieurs hiérarchiques. En Corée, la Commission de règlement des litiges relatifs à l'environnement et la Commission des recours administratifs ont été en outre créées pour gérer divers litiges entreprises-administration et consommateurs-administration dans le domaine de l'environnement.

Conclusions

Les réponses au questionnaire soulignent la disparité des règles régissant le RAL. Des règles différentes ont été élaborées dans des contextes distincts. Dans un certain nombre de secteurs, le cadre juridique existant offre une ligne de conduite aux parties éventuelles à une procédure de RAL au niveau national. De nombreux pays réglementent par exemple l'offre de services d'arbitrage. Peu de réglementations régissent en revanche l'offre de types moins formels de RAL entre entreprises et consommateurs. La réglementation en place concerne généralement l'offre de RAL par des mécanismes créés, financés ou gérés par l'État.

L'OCDE s'est principalement attachée aux mécanismes de RAL souples et informels, conçus pour l'environnement en ligne. Aucun pays membre n'a mentionné à cet égard l'existence de dispositions juridiques spécifiques, bien que la plupart d'entre eux aient exprimé leur intérêt pour la promotion d'un RAL juste et efficace spécialisé dans les litiges en ligne entre entreprises et consommateurs d'un faible montant, notamment les litiges transfrontières. Au niveau transfrontière, on voit par ailleurs apparaître clairement des différences nationales pour les aspects suivants : validité des dispositions contractuelles de soumission des litiges au RAL, principes procéduraux à utiliser au cours du RAL, confidentialité et sécurité des procédures, validité des accords issus d'un RAL et existence de mécanismes d'exécution.

Les Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique suggèrent que le RAL offre un moyen de régler les problèmes des consommateurs dans le cadre du commerce électronique. Les divergences nationales entre les cadres juridiques actuels applicables au RAL peuvent avoir des conséquences sur la mise en œuvre du RAL dans le contexte transfrontière. Les pays membres, les entreprises et les consommateurs doivent savoir quel est le type de dispositifs de RAL offerts dans les différents pays et connaître les règles qui les régissent. Ce document est très utile de ce point de vue.

NOTES

1. Le principal instrument juridique relatif au RAL pour les litiges en ligne est la directive européenne (2000/31/CE) sur le commerce électronique. Il encourage le RAL pour ce type de litiges, mais ne s'accompagne d'aucune obligation juridique.
2. Les pays membres de l'OCDE ont en outre adopté des lignes directrices relatives à la protection des consommateurs en ligne prévoyant un accès effectif à un RAL juste et diligent, sans frais ni entraves inutiles.
3. Article 17 de la loi du 6 juillet 1989 relative au bail des locaux à usage d'habitation.
4. Règlement de procédure civile du Maine, Règle 16B.
5. Article 615 du Code de procédure civile fédérale.
6. L'*Alternative Dispute Resolution Act* stipule que les tribunaux ne peuvent pas imposer aux parties le RAL après l'introduction de l'action si le litige se fonde sur des droits constitutionnels, concerne la protection de l'égalité des droits ou le droit de vote ou si la réparation recherchée consiste en dommages-intérêts d'un montant supérieur à USD 150 000.
7. Article 9 du décret du 20 mars 1978.
8. Pour les procédures d'arbitrage, voir le Code de procédure civile, art. 1065.1.e et pour les procédures d'avis contraignant, voir le Code civil titre 7, art. 902.
9. Aux États-Unis, les spécialistes du RAL travaillent actuellement à la rédaction d'un projet de loi uniforme sur la médiation, exigeant d'une manière générale la confidentialité des médiations, mais avec une liste d'exceptions précises : la renonciation, les communications relatives à la perpétration actuelle ou future d'une infraction, l'enregistrement d'un accord signé, les réunions et les documents légalement ouverts au public et les médiations d'intérêt général, la preuve de maltraitance ou de négligence vis à vis d'un enfant, la preuve d'une faute professionnelle ou autre du médiateur, la preuve d'une faute professionnelle ou la faute de l'une des parties ou de l'un de ses représentants.
10. En Nouvelle-Zélande, l'*Arbitration Act* de 1996 interdit la divulgation des informations révélées au cours d'un arbitrage, sauf si les parties y consentent.
11. Voir le projet de loi uniforme sur la médiation cité plus haut.
12. Pour les États-Unis, voir www.adr.org; www.arb-forum.com.
13. Voir la loi relative à la protection et à la défense des usagers des services financiers.
14. Loi n° 580 du 29/12/1993.
15. Loi relative à la promotion de l'utilisation des réseaux d'information et de communication et à la protection des informations (modifiée le 16 janvier 2001).
16. Créée sous l'égide du ministère de l'Information et de la Communication.
17. Le *Privacy Act* de 1993.
18. Le poste de Commissaire à la protection de la vie privée est financé par l'État, mais sa structure est celle d'une entité de la Couronne indépendante.
19. L'*Administrative Appeals Tribunal Act* de 1975 du Commonwealth et législation relative aux droits de l'homme.

APPENDICE

QUESTIONNAIRE SUR LES DISPOSITIONS JURIDIQUES LIÉES AU RÈGLEMENT ALTERNATIF DES LITIGES ENTRE ENTREPRISES ET CONSOMMATEURS RELATIFS A LA VIE PRIVÉE ET A LA PROTECTION DES CONSOMMATEURS

Les gouvernements sont invités à répondre aux questions sur les éventuelles « dispositions juridiques » en indiquant l'ensemble des législations ou réglementations nationales, y compris les décisions judiciaires (jurisprudence) ou conventions, traités ou autres instruments juridiques internationaux, auxquels leur pays est partie.

Les acteurs non gouvernementaux sont invités à répondre aux questions sur les éventuelles « dispositions juridiques » en indiquant l'ensemble des législations ou réglementations nationales, y compris les décisions judiciaires (jurisprudence) ou conventions, traités ou autres instruments juridiques internationaux dont ils ont connaissance.

Questions

Dans vos réponses aux questions ci-après, veuillez :

- Traiter principalement le règlement alternatif des litiges (RAL) entre entreprises et consommateurs. Toutefois, lorsque c'est utile pour cet environnement, les réponses peuvent couvrir aussi d'autres formes de RAL, comme les systèmes alternatifs d'entreprise à entreprise, de consommateur à consommateur, d'entreprise à administration et de consommateur à administration.
- Traiter de l'ensemble des dispositions juridiques, mais plus particulièrement de celles qui concernent la vie privée et la protection des consommateurs.
- Traiter principalement des mécanismes de RAL entre entreprises et consommateurs (comme la négociation assistée et la médiation) ; toutefois, il est possible de traiter dans les réponses de l'arbitrage entre entreprises et consommateurs dans les cas où cela se justifie.
- Distinguer le cas échéant les dispositions juridiques qui visent le RAL entre entreprises et consommateurs en général, les dispositions juridiques qui visent le RAL entre entreprises et consommateurs au niveau sectoriel et les dispositions juridiques qui peuvent ne pas mentionner le RAL, mais pourraient néanmoins avoir une incidence sur le RAL (en particulier pour les litiges concernant la vie privée et la protection des consommateurs).
- Indiquer toute différence entre l'utilisation du RAL entre entreprises et consommateurs pour les litiges intervenant dans un contexte national par opposition à ceux qui comportent un élément transfrontière.

De plus, nous vous rappelons que nous utilisons l'expression « dispositions juridiques » dans son acceptation générale la plus large.

A. Dispositions spécifiques au RAL

1. Existe-t-il des dispositions juridiques qui concernent spécifiquement le RAL entre entreprises et consommateurs (couvrant le RAL entre entreprises et consommateurs soit de façon générale, soit sur une base sectorielle) ? Dans l'affirmative, veuillez décrire ces dispositions.

2. Existe-t-il des dispositions juridiques qui visent spécifiquement d'autres formes de RAL (de façon soit générale, soit sectorielle), comme les mécanismes de RAL d'entreprise à entreprise, de consommateur à consommateur, d'entreprise à administration ou de consommateur à administration ? Dans l'affirmative, veuillez décrire ces dispositions.

B. Recours au RAL

3. Existe-t-il des dispositions juridiques qui empêcheraient ou interdiraient le recours au RAL pour certains types ou certaines catégories de litiges ?[1] Dans l'affirmative, veuillez expliquer ces dispositions et leur application.

4. Existe-t-il des dispositions juridiques qui imposeraient ou encourageraient le recours au RAL pour certains types ou certaines catégories de litiges ? Dans l'affirmative, veuillez expliquer ces dispositions et leur application.

C. Épuisement des voies de recours par le RAL

5. Un accord contractuel entre les parties (par exemple entre une entreprise et un consommateur) prévoyant le recours à un mécanisme de RAL avant la saisine des tribunaux serait-il en contradiction avec une quelconque disposition juridique ? Dans l'affirmative, veuillez donner les références de ces dispositions.

6. Existe-t-il des dispositions juridiques qui imposeraient aux parties ou exigeraient d'elles de recourir d'abord à un mécanisme de RAL avant la saisine d'un tribunal ? Dans l'affirmative, veuillez donner les références de ces dispositions.

D. RAL contractuellement contraignant

7. Existe-t-il des dispositions juridiques qui empêcheraient ou interdiraient un accord contractuel entre les parties (par exemple entre une entreprise et un consommateur) prévoyant qu'elles sont liées par la décision produite par le RAL, si l'accord contractuel :

a. Est antérieur au litige ?
b. Postérieur au litige, mais préalable à l'engagement de la procédure de RAL ?
c. Intervient à la fin de la procédure de RAL (transaction) ?

8. Existe-t-il des dispositions juridiques qui encourageraient ou autoriseraient explicitement un accord contractuel entre les parties (par exemple entre une entreprise et un consommateur) prévoyant qu'elles sont liées par la décision produite par le RAL, si l'accord contractuel :

a. Est antérieur au litige ?
b. Postérieur au litige, mais préalable à l'engagement de la procédure de RAL ?

---

1. Par exemple, un domaine peut-être envisageable serait celui des litiges impliquant un préjudice important pour un utilisateur ou un consommateur, comme une grave violation de la vie privée, un préjudice corporel ou la perte d'une importante somme d'argent.

c. Intervient à la fin de la procédure de RAL (transaction) ?

9. Si les parties peuvent convenir d'être liées, existe-t-il des dispositions juridiques qui pourraient empêcher ou interdire, en totalité ou en partie, la mise en œuvre des décisions issues de la procédure de RAL ?[2] Veuillez indiquer dans quelles circonstances cela pourrait se produire.

E. Exécution judiciaire

10. Une décision de RAL peut-elle être rendue exécutoire par une instance judiciaire ? Dans quelles circonstances ?

F. Procédure

11. Existe-t-il des dispositions juridiques qui imposeraient la mise en place de certaines garanties procédurales[3] lors d'une procédure de RAL ?

a. De façon générale ?
b. Concernant des droits spéciaux, ou particuliers, des consommateurs ou utilisateurs ?
c. Concernant des droits spéciaux, ou particuliers, des entreprises ?

G. Confidentialité

12. Si les parties et le prestataire du service de RAL conviennent de garder confidentielles les informations relatives à une procédure et/ou une décision de RAL, existe-t-il des dispositions juridiques imposant leur divulgation dans certaines circonstances ? Dans l'affirmative, lesquelles ?

H. Services de RAL

13. Existe-t-il des dispositions juridiques définissant les conditions requises pour pouvoir proposer des services de RAL entre entreprises et consommateurs ?

14. Existe-t-il des dispositions juridiques définissant les conditions requises pour pouvoir servir de tiers impartial dans une procédure de RAL ?

15. Existe-t-il d'autres dispositions juridiques concernant l'activité des fournisseurs de services de RAL, notamment le coût du RAL pour, soit les utilisateurs et consommateurs, soit les entreprises ?

I. Autres aspects

16. Existe-t-il d'autres obligations ou restrictions juridiques applicables au RAL qui n'ont pas été abordées plus haut ?[4]

---

2. Par exemple, les dispositions de l'article 5 de la Convention de Rome pourraient-elles affecter l'obligation pour un consommateur d'exécuter une décision ?

3. Ces garanties procédurales peuvent être notamment la transparence, la diligence, l'accessibilité et la modicité des coûts, la possibilité d'être représenté par un juriste, la garantie d'une procédure contradictoire et l'indépendance ou l'impartialité du prestataire du service de RAL.

4. Veuillez par exemple traiter les engagements ou accords gouvernementaux, y compris les recommandations administratives, ou les autres éléments susceptibles d'affecter de manière significative la compréhension de l'importance et de la nature de l'incidence des dispositions juridiques en vigueur sur le RAL.

Chapitre 10

RÉSOLUTION EN LIGNE DES LITIGES LIÉS AU COMMERCE ÉLECTRONIQUE : RÈGLEMENT ALTERNATIF DES LITIGES (RAL) – LES QUESTIONS A SE POSER

A l'origine, ce chapitre a été conçu comme un outil pédagogique qui permettrait aux utilisateurs individuels de déterminer si la RAL en ligne était susceptible de les aides à résoudre un litige : à quoi il faut réfléchir avant de considérer la RAL, comment choisir une modalité particulière de RAL, où trouver des fournisseurs de RAL et ce qu'il faut faire si la RAL ne peut pas résoudre le différend.

Chapitre 10

RÉSOLUTION EN LIGNE DES LITIGES LIÉS AU COMMERCE ÉLECTRONIQUE : RÈGLEMENT ALTERNATIF DES LITIGES (RAL) – LES QUESTIONS A SE POSER

Pourquoi acheter en ligne ? Pour une multitude de raisons : opportunités, commodité, choix, prix compétitifs, information. Mais savez-vous ce qui se passerait en cas de problème ? Imaginez que vous ne recevez pas les biens commandés, ou qu'ils vous arrivent endommagés : quels seraient vos recours ?

Bien souvent, lorsque vous êtes en ligne, les moyens prévus par le vendeur pour résoudre d'éventuels problèmes sont indiqués sur le site Web. Certaines entreprises publient leur politique en matière de règlement des litiges. En tant que consommateur, il vous appartient de vérifier l'existence d'un service de réclamation, ou d'une garantie de remboursement. Il faut au moins vous assurer que le site comporte un numéro de téléphone ou une adresse électronique qui permette de contacter la société en cas de problème. De plus, certains vendeurs en ligne participent à des programmes de « sceau » ou « marque de confiance » qui attestent que l'entreprise respecte certaines normes. Pour en savoir plus il suffit de cliquer sur le sceau ou la marque de confiance. Quelques entreprises proposent des services de compte séquestre, qui consiste à confier l'argent à un tiers jusqu'à ce que les biens ou les services que vous avez commandés vous aient été fournis. D'autres proposent un système d'assurance vous permettant de vous faire rembourser si vous n'obtenez pas les biens ou les services commandés.

En cas de problème lors d'un achat en ligne, la première chose à faire est de tenter de le régler directement avec le vendeur. Si vous n'y parvenez pas, peut-être pensez-vous que la seule solution est d'engager des poursuites judiciaires. Pourtant, il existe souvent une option plus rapide et moins onéreuse pour résoudre votre litige : le recours à un tiers neutre. Cette procédure, de plus en plus utilisée par les consommateurs et les commerçants en ligne, s'appelle le Règlement alternatif des litiges (RAL). Vous contactez un prestataire de RAL, vous déposez votre réclamation en ligne, l'autre partie vous répond en ligne et le litige est résolu sans que vous ayez eu à quitter votre fauteuil, et pour un coût minime. Il faut savoir qu'un certain nombre de sites prévoient un recours obligatoire à cette procédure avant tout dépôt de plainte devant les tribunaux ; d'autres exigent que vous renonciez à toute action en justice. Il est donc important de vérifier avant tout les conditions et modalités de la vente. Ensuite, renseignez-vous auprès de votre association de consommateurs pour savoir si les dispositions de RAL « obligatoire » ou « exécutoire » sont légales dans votre pays.

Si vous ne souhaitez pas renoncer à tout droit de poursuite, il est peut-être avisé de ne pas acheter sur un tel site. Voici les questions à se poser pour déterminer si le RAL peut apporter une solution à votre litige.

Questions-clés
1) Quels sont les points à éclaircir avant d'envisager le RAL ?
2) Quels types de RAL en ligne puis-je utiliser ?
3) Que type de RAL choisir ?
4) Comment choisir mon fournisseur de RAL ?
5) Comment trouver des fournisseurs de RAL qui peuvent m'aider?
6) Et si le RAL n'est pas la solution ?

1) Quels sont les points à éclaircir avant d'envisager le RAL?

TIP 1

Avant de recourir au RAL, posez-vous les questions suivantes :

Quelles seraient les solutions satisfaisantes pour moi?

Il faut savoir clairement quelles solutions vous considéreriez comme acceptables : Voulez-vous un remboursement ? Voulez-vous que le bien en question soit remplacé ? Voulez-vous que le vendeur prenne un autre mesure ?

Ai-je tenté moi-même de résoudre le problème avec le commerçant ?

Généralement, la meilleure chose à faire en premier lieu est de contacter directement l'entreprise. Les entreprises ont souvent un excellent système de traitement des réclamations qui peut proposer une solution rapide et efficace à votre problème.

Puis-je obtenir de l'aide de l'émetteur de ma carte de paiement ?

TIP 2

Si vous avez payé des biens ou des services à l'aide d'une carte de paiement ou de crédit, vous bénéficiez peut-être à ce titre de protections particulières. Lisez attentivement les relevés de votre carte de paiement, où vous trouverez des informations sur les modalités d'opposition, et demandez à votre association de consommateurs s'il existe des protections particulières dans votre pays.

Est-ce que je suspecte une fraude ou pratiques ?

Dans ce cas, contactez votre association de consommateurs ou les autorités chargées de la protection des données.

TIP 3

2) Quels sont les types de RAL disponibles en ligne ? TIP 4

La médiation et l'arbitrage sont déjà des modes de règlement assez connus et d'un usage courant dans le commerce traditionnel et sont de plus en plus utilisé en ligne. La négociation automatisée est une nouvelle forme de RAL qui tire particulièrement bien parti des avantages de l'environnement en ligne.

Qu'est-ce que la médiation?

Dans la médiation, un tiers neutre, le médiateur, vous aide, vous-même et l'autre partie, à résoudre le problème en facilitant le dialogue. Toutefois, il appartient aux deux parties de parvenir à un accord. D'autres noms donnés à ce type de RAL sont notamment la « négociation assistée », la « facilitation » et la « conciliation ».

Qu'est-ce que l'arbitrage ?

L'arbitrage est une procédure dans laquelle intervient un tiers neutre – l'arbitre – qui s'informe auprès de vous et de l'autre partie et rend une décision. Sa décision a souvent force exécutoire.

Qu'est-ce que la négociation automatisée ?

Il s'agit d'un processus informatisé qui a pour principal objectif de résoudre les litiges portant sur des montants d'argent. Il repose souvent sur un système d'enchères à l'aveugle, dans lequel chaque partie fait des offres successives afin de parvenir à un accord, sans savoir ce qu'a proposé l'autre partie. Le processus arrive à son terme lorsque les offres sont suffisamment proches et que l'ordinateur propose une solution. Il est vivement conseillé de lire attentivement les conditions et modalités de la négociation automatisée avant d'y recourir car la solution générée par l'ordinateur a souvent force contractuelle exécutoire.

3) Comment choisir une forme particulière de RAL?

Un certain nombre de commerçants en ligne précisent dans leurs conditions de vente qu'en cas de litige au sujet de la transaction, il sera fait usage d'un certain type de RAL. Il vous appartient de lire attentivement ces conditions de vente et de décider si elles vous conviennent on non avant d'acheter. Avec d'autres commerçants, vous êtes libre de lancer vous-même la procédure de RAL. Pour choisir le type de RAL qui se prêterait le mieux à votre litige, posez-vous les questions suivantes.

Quel rôle doit jouer le tiers ?

Dans l'arbitrage, le tiers prend la décision. Dans la médiation, le rôle du tiers peut varier mais votre rôle actif est essentiel pour proposer des compromis et trouver des solutions. Dans la négociation automatisée, une solution est générée par un programme informatique.

Le tiers doit-il avoir des qualifications ou une expertise particulières ?

Les arbitres et les médiateurs ont parfois des qualifications officielles. Si votre litige est extrêmement technique, ou qu'il nécessite une expertise particulière, il est important de veiller à ce que le tiers ait l'expertise suffisante dans le domaine pertinent. S'il s'agit d'un litige simple dans lequel, par exemple, vous et l'entreprise êtes en désaccord sur les faits, des qualifications précises sont généralement moins indispensables. Dans un cas comme dans l'autre, il peut être utile que le tiers ait une certaine expérience dans le domaine sur lequel porte le litige.

Est-ce que je souhaite que la décision ait un caractère contraignant ? TIP 5

Vous pouvez être tenu d'obéir à une décision par arbitrage. En d'autres termes, il est possible que cette procédure vous interdise tout autre recours, – notamment de poursuivre le commerçant en justice. Toutefois, dans certains pays, les consommateurs ne peuvent pas abandonner le droit d'ester en justice. Informez-vous auprès de votre association de consommateurs ou de protection des données.

4) Comment choisir un fournisseur de RAL ?

Examiner les points suivants :

Le fournisseur adhère-t-il à un code de conduite ou à des lignes directrices ?

Un fournisseur de RAL peut se référer à un ensemble de lignes directrices ou à un code de conduite. Cela signifie généralement qu'il s'est volontairement engagé à respecter certaines règles. Le site web du fournisseur de RAL vous renseignera sur ce type de mesures.

Que coûte ce programme RAL ?

Certains programmes sont gratuits. D'autres sont facturés un montant forfaitaire ou un pourcentage en fonction de votre capacité à payer. Consultez les sites du commerçant et du fournisseur du RAL pour savoir qui paiera les coûts afférents au RAL.

Quelle est la durée de la procédure ? TIP 6

C'est variable. Le RAL est souvent beaucoup plus rapide qu'une action en justice.

Puis-je suivre la procédure dans ma langue ?

Demandez si vous pouvez suivre la procédure dans votre langue. Des services de traduction existent parfois, mais informez-vous pour savoir si un traducteur est disponible et informez-vous également sur les prix.

Sous quelle forme vais-je présenter mon affaire ? TIP 7

La communication elle-même peut se faire selon différentes formes : il peut s'agir d'un simple échange de messages électroniques, ou toutes les parties peuvent être « présentes » grâce à des webcams. Les points suivants sont à prendre en considération :

Temps : S'il s'agit d'un problème complexe, vous aurez peut-être besoin d'un délai de réflexion avant de répondre.

Technologie : Vous pouvez sans difficulté envoyer un message électronique de chez vous, mais êtes vous équipé pour la visioconférence ?

Sécurité : Les messages envoyés par courrier électronique ne comportent pas de dispositifs de sécurité particuliers. Le niveau de sécurité souhaitable dépend du caractère sensible de l'information envoyée. La plupart des litiges portant sur de petits montants ne nécessitent pas de dispositifs particuliers de sécurité, mais il faut veiller à ne jamais envoyer d'informations personnelles hautement sensibles dans un message électronique. Si le litige lui-même suppose l'échange d'informations personnelles

hautement sensibles, il serait peut-être bon de recourir à un prestataire de RAL qui propose des pages web sécurisés pour transmettre les informations.

Le professionnel du RAL a-t-il pris des engagements en matière de protection de la vie privée ?

Le prestataire est-il engagé par une déclaration de protection des données personnelles, ou indique-t-il comment seront utilisées vos données personnelles ? Il peut arriver que le fournisseur de RAL vous demande votre consentement pour publier une relation non nominative de votre affaire, afin d'aider d'autres clients à décider s'ils souhaitent recourir à un fournisseur de RAL particulier, et d'éclairer ceux qui se trouveraient dans des situations comparables sur les issues possibles de leur cas.

5) Comment trouver des fournisseurs de RAL pour m'aider ? TIP 8

Il existe plusieurs annuaires de fournisseurs de RAL que vous pouvez consulter.

6) Et si le RAL n'est pas la solution ?

Si une démarche de RAL ne vous a pas permis d'obtenir satisfaction, ou si vous avez décidé de ne pas tenter cette pratique, votre seul recours est peut-être l'action en justice.

ASTUCES

1. Ces questions concernent le problème de la résolution des différends. Mais avant toute transaction ou interaction avec un site web, beaucoup d'autres éléments importants sont à prendre en considération. Il faut penser notamment à la protection des données personnelles. On trouvera à l'adresse suivante des liens vers des sources d'information en ligne concernant la protection de la vie privée: http://cs3-hq.oecd.org/scripts/pwv3/privcontacts.htm. Il faut également envisager la question de la protection des consommateurs. Pour en savoir plus sur les protections à attendre lorsque l'on achète en ligne, voir la page : www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html. Pour des informations complémentaires sur la consommation en ligne sans risque, voir : www.econsumer.gov/english/contentfiles/shoptips_1.html.

2. L'OCDE a préparé un ensemble de *Questions courantes* sur l'utilisation de cartes de crédit en ligne et les protections existant en cas de problème : www.oecd.org/sti/consumer-policy. Pour une liste d'associations de consommateurs, voir la page : www.oecd.org/countrylist/0,2578,en_2649_34267_1783507_1_1_1_1,00.html.

3. Pour engager une action transnationale en justice concernant un problème de protection du consommateur ou des données personnelles, voir la page www.econsumer.gov. Pour accéder à des sources d'information en ligne concernant la protection de la vie privée, visiter la page ressources de l'OCDE : http://cs3-hq.oecd.org/scripts/pwv3/ privcontacts.htm.

4. Tous les pays de l'OCDE ne retiennent pas la même classification et les mêmes définitions des différentes formes de RAL. Il se peut que des formes de RAL particulières existent dans votre pays auxquelles vous pouvez recourir.

5. Des liens vers des autorités de protection des consommateurs sont disponibles à : www.oecd.org/countrylist/ 0,2578,en_2649_34267_1783507_1_1_1_1,00.html. Des liens vers des autorités de protection des données personnelles sont disponibles à : http://cs3-hq.oecd.org/scripts/pwv3/ privcontacts.htm.

6. S'agissant de la question des délais, il faut savoir qu'il existe dans la plupart des pays de l'OCDE des délais légaux pour intenter une action. Assurez-vous que la procédure de RAL sera achevée en temps voulu pour vous permettre de poursuivre en justice si c'est nécessaire.

7. Pour savoir si les informations que vous fournissez sont sécurisées, assurez-vous que l'adresse web du formulaire de RAL commence bien par « https: », et non par « http: », et qu'un symbole au bas de l'écran (clé ou cadenas fermé, par exemple) signale que votre transaction sera sécurisée.

8. La Commission européenne a réuni des informations sur les fournisseurs de RAL dans le cadre du projet EJE-Net ; on les trouvera à : http://europa.eu.int/comm/consumers/redress/out_of_court/eej_net/index_en.htm. Consumers International a réalisé une évaluation de plusieurs fournisseurs de services de RAL. Les résultats sont consultables à l'adresse : www.consumersinternational.org/document_store/Doc35.pdf.

Chapitre 11

LE RESPECT ET LA MISE EN ŒUVRE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CONTEXTE DU COMMERCE ÉLECTRONIQUE

Ce rapport présente et examine les mécanismes disponibles dans les pays membres de l'OCDE pour faire face au manque de respect des principes et des politiques en matière de vie privée et pour assurer des possibilités de recours. Il a pour objectif de servir de point de départ pour évaluer l'application pratique des instruments existants de respect et de mise en œuvre dans un environnement de réseaux et de leur conformité avec les objectifs des les Lignes directrices de l'OCDE en matière de vie privée, notamment en ce qui concerne leur efficacité et leur applicabilité dans différentes juridictions.

Chapitre 11

LE RESPECT ET LA MISE EN ŒUVRE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CONTEXTE DU COMMERCE ÉLECTRONIQUE

Introduction

Le respect des principes de protection des données privées et la mise en œuvre de ces principes sont des concepts distincts mais interdépendants. En effet, le respect renvoie au niveau d'adhésion aux dispositions législatives, alors que la mise en œuvre recouvre les mécanismes coercitifs qui peuvent être utilisés pour contraindre à cette adhésion et pour défendre les droits des personnes lésées en cas de violation. Cela étant, l'un et l'autre sont intimement liés car plus le respect est assuré moins les mécanismes coercitifs ont d'importance ; à l'inverse, l'existence de mécanismes de contrôle stricts incite les acteurs à un meilleur respect des règles. Dans ce rapport, compte tenu de la relation étroite existant entre respect et mis en œuvre, ces deux aspects ont été traités ensemble, tout en tenant compte de ce qui peut les séparer.

Contexte

Le 12 mars 2002, un Questionnaire sur le respect des règles de protection de la vie privée et sur leur mise en œuvre dans le contexte du commerce électronique entre entreprises et consommateurs a été adressé aux gouvernements de l'OCDE et à des acteurs du secteur privé. Ce questionnaire avait été élaboré dans le cadre du programme de travail du Groupe de travail sur la sécurité de l'information et la vie privée (WPISP) du Comité PIIC dans la perspective des objectifs de la Déclaration ministérielle de l'OCDE sur la protection des données privées sur les réseaux mondiaux, publiée lors de la Conférence ministérielle d'Ottawa d'octobre 1998. Dix-neuf pays membres et trois organisations représentant le secteur privé ont envoyé leurs réponses.

Dans cette déclaration, les Ministres s'engagent à garantir l'existence de mécanismes efficaces de mise en œuvre permettant à la fois de régler les problèmes de non-respect des principes et des politiques de protection des données privées, et de garantir l'accès à des moyens de réparation. La Déclaration appelle en outre l'OCDE à « promouvoir l'éducation et la sensibilisation des utilisateurs aux problèmes de respect des données privées en ligne et aux moyens dont ils disposent pour protéger leur vie privée sur les réseaux mondiaux ».

Depuis la Conférence ministérielle de l'OCDE, le respect et la mise en œuvre des normes constituent les principaux axes de travail en matière de protection des données privées. Devant les insuffisances des démarches purement législatives et réglementaires, les gouvernements et le secteur privé élaborent d'autres méthodes pour assurer le respect et la mise en œuvre. Ces méthodes s'appuient sur l'autorégulation, les incitations relevant du marché, ainsi que sur des moyens technologiques et autres qui vont au-delà des approches réglementaires classiques, et qui sont mieux adaptées au commerce électronique, univers qui ne connaît pas de frontières et qui évolue constamment. Le moment était donc venu de faire le point sur les mécanismes utilisés dans les pays membres de l'OCDE pour assurer le respect et la mise en œuvre, et de se demander si ces mécanismes étaient bien adaptés aux exigences du commerce électronique.

Les répondants étaient invités à fournir des informations factuelles simples et non à procéder à une analyse détaillée. Les gouvernements devaient répondre aux questions concernant d'éventuelles

« dispositions législative », ce qui recouvre les lois et règlements nationaux, les décisions de justice (jurisprudence), ainsi que les conventions, traités ou autres instruments législatifs internationaux. Le questionnaire portait sur les instances gouvernementales (ministères, par exemple), et sur les instances indépendantes (autorités de protection des données) ; dans cette étude, le terme « agence gouvernementale » renvoie à ces deux types d'entités.

La participation du secteur privé était également sollicitée, car les entreprises peuvent apporter des enseignements sur leur expérience pratique, en mettant en lumière la démarche qu'elles suivent pour mettre en œuvre les dispositifs de protection des données. Par conséquent, les représentants d'entreprises étaient invités, non seulement à donner des informations sur les dispositions législatives, mais aussi à décrire les solutions d'autorégulation dont ils ont connaissance, comme les programmes de sceaux de certification ou de marques de fiabilité, la nomination de responsables internes de la confidentialité des données privées, les dispositifs de mise en œuvre mis en place par les organisations professionnelles, etc., comme décrit dans le questionnaire. Ce rapport présente un panorama général de la question. Il s'appuie sur les réponses reçues et ne comporte aucun jugement.

I. Synthèse des réponses

Voici la liste des pays membres et des organisations professionnelles qui ont répondu au questionnaire : Allemagne, Australie, Autriche, Belgique, Corée, Finlande, France, États-Unis, Italie, Japon, Mexique, Norvège, Pays-Bas, République slovaque, République tchèque, Royaume-Uni, Suède, Suisse, Turquie, fournisseurs d'accès Internet (FAI) de la République slovaque, *US Council for International Business* (USCIB) et *US Direct Marketing Association* (DMA).

Normes et instruments

Législations en matière de vie privée

Parmi les pays où une loi de protection des données privées d'application générale existe, citons l'Allemagne, l'Australie, l'Autriche, la Belgique, la Corée, la Finlande, la France, l'Italie, la Norvège, la République slovaque, la République tchèque, le Royaume-Uni, la Suède et la Suisse. Les pays dépourvus de loi d'application générale sont notamment les États-Unis, le Japon, le Mexique et la Turquie. Le Japon et la Turquie envisagent actuellement de se doter d'une telle législation. Certains pays ont aussi des législations sectorielles. Par exemple, chez certains membres de l'Union européenne (UE), il existe une législation sectorielle de protection des données privées dans les télécommunications ; ainsi la Finlande est dotée de lois sur les télécommunications, l'ouverture des activités de l'État, la protection des données privées au travail, les fichiers de police et les casiers judiciaires. Aux États-Unis, il existe des lois de protection des données à caractère personnel dans différents secteurs : protection des données concernant les enfants, des informations financières et médicales. En Allemagne, il existe des lois spécifiques applicables aux services en ligne. La plupart des répondants font également état d'autres formes de régulation légale : décrets, ordonnances, règlements administratifs et jurisprudence (par exemple, les décrets ou les ordonnances existent en Allemagne, en France, en Italie, en Suède et en Suisse). Le rôle de la jurisprudence varie selon les pays membres. Aux États-Unis, par exemple, c'est une source du droit importante, alors que la France ne la considère pas comme une source autonome du droit. Au Japon, plusieurs lignes directrices d'autorégulation sont en place, alors qu'au Royaume-Uni, la législation des droits de l'homme occupe une place centrale. Les États-Unis reconnaissent une place importante aux règles et règlements administratifs.

Instruments internationaux et régionaux

Les pays membres de l'Union européenne sont liés par la Directive sur la protection des données[1] et un certain nombre de dispositifs et instruments de droit public conclus par la Commission européenne (comme l'Accord UE/États-Unis de la sphère de sécurité[2] et les contrats-types de transfert de données[3]. Quelques pays européens sont aussi parties à d'autres accords de l'Union européenne qui comprennent des dispositions en matière de protection des données, notamment dans le domaine de la coopération policière[4]. Ces mêmes pays figurent également parmi les membres du Conseil de l'Europe et sont liés par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[5]. Le Mexique a signé un Accord de partenariat économique, de coordination politique et de coopération avec la Communauté européenne et ses États membres, ce qui l'engage notamment à promouvoir la protection des données à caractère personnel. Les répondants partagent également l'engagement de mettre en œuvre différents instruments internationaux comme les Lignes directrices de l'OCDE régissant la protection des données privées et les flux transfrontières de données à caractère personnel (Lignes directrice de l'OCDE sur la vie privée) et les Principes directeurs de l'ONU pour la réglementation des fichiers personnels informatisés, entre autres).

S'agissant précisément des contrats-types de transfert de données, les décisions de la Commission européenne sur les contrats-types s'appliquent dans les États membres de l'UE, qui les ont mises en œuvre. La République tchèque recommande leur utilisation. L'USCIB a participé à la rédaction d'autres contrats types que la Chambre de commerce internationale (CCI) et d'autres organisations professionnelles ont récemment soumis à l'approbation de la Commission européenne[6]. Un ensemble de contrats-types a également été publié conjointement par la CCI, la Commission européenne et le Conseil de l'Europe[7].

Codes de conduite, programmes de marques de confiance, etc.

Dans la plupart des pays, il n'existe pas de codes de conduite avalisés par l'État. En Australie, des recueils de pratiques ont été soumis au *Privacy Commissioner* pour approbation. En République slovaque, toutes les normes technologiques doivent être approuvées par un organisme public, et en Suède, les organisations professionnelles peuvent soumettre des codes de conduite pour avis au Conseil d'inspection des données ; à cette date, le Conseil a émis un avis sur deux de ces codes. Le Japon a créé un modèle pour les lignes directrices à établir par les organisations professionnelles, et plusieurs entreprises ont élaboré des lignes de conduite conformément à ce modèle. Dans de nombreux pays (comme l'Autriche, les États-Unis, la France et le Mexique), l'utilisation de codes de conduite pour la protection des données privées est encouragée.

La majorité des répondants déclarent qu'il existe dans leur pays des codes de conduite sectoriels privés, des pratiques exemplaires ou des programmes de sceau de confidentialité ou de marques de confiance entérinés par des associations professionnelles, ou largement reconnus par l'ensemble des entreprises ou par un secteur particulier. La plupart des réponses concernent des codes de conduite, mais dans certains pays (Allemagne, États-Unis et Japon, par exemple) il existe également des programmes de sceau de confidentialité ou de marque de confiance. En Corée, l'Association sur l'information et les télécommunications indique qu'elle décerne un sceau *ePrivacy* aux sites Internet pertinents qui obéissent à des critères stricts en matière de protection de données.

Sécurité

La quasi-totalité des répondants disent qu'il existe une forme de régulation gouvernementale applicable à la sécurité des sites Web, mais dans beaucoup d'entre eux (notamment l'Autriche, la Finlande, la France, la Norvège et la Suède) il n'existe pas de législation spécifique aux sites Web mais une

législation générique sur la protection ou la sécurité des données. Au Japon, des lignes directrices sectorielles destinées aux entreprises établissent des paramètres de sécurité ; d'autres lignes directrices ont également été édictées par des organismes publics. Au Mexique, il existe des mesures d'autorégulation dans le secteur financier qui garantissent la sécurité des services en ligne. Aux États-Unis, un site Web qui induit l'internaute en erreur sur ses pratiques en matière de protection de la vie privée et de sécurité peut être en infraction avec le droit fédéral de protection des consommateurs. Il existe également des dispositions législatives et des règlements administratifs en matière de normes de sécurité applicables au secteur financier.

Respect des règles

Variété des dispositifs

Les réponses reçues font état de la grande variété des organismes que l'on peut consulter pour information et avis sur le respect des normes citées précédemment. Les pays qui sont dotés d'une autorité indépendante de protection des données privées (l'Australie, l'Autriche, la Belgique et la République tchèque, par exemple) indiquent que cette autorité peut être consultée. Plusieurs répondants (comme la Finlande) mentionnent également les avocats et cabinets d'avocats privés. Quelques-uns citent des organes publics autres que les responsables de la confidentialité des données privées ; le Japon, par exemple, indique qu'il existe dans chaque préfecture de police des « conseillers sur la sécurité de l'information », qui dispensent informations et conseils sur les « lois relatives aux accès illicites à des ressources informatiques » et sur la criminalité informatique.

Pratiques exemplaires, outils logiciels, etc.

Les répondants indiquent que les autorités gouvernementales chargées de la protection des données privées peuvent examiner les pratiques des entreprises en matière de données privées. Il peut s'agir de procédures administratives, d'examens fondés sur les pratiques exemplaires ou s'appuyant sur des outils logiciels, ou d'autres moyens d'analyse des pratiques des entreprises exerçant des activités en ligne. Le Japon indique qu'il existe des pratiques standard (comme le JIS Q 15001) qui prévoient des audits réguliers des entreprises, ainsi qu'un système de notation de la protection des données privées. La Suisse mentionne une initiative du secteur privé : un label de qualité des sites Web associé à un audit des sites de commerce électronique. Au Royaume-Uni, le *British Standards Institute* a publié un manuel d'auto-examen des pratiques et a intégré un module de protection des données dans sa suite d'outils logiciels de mise en conformité juridique. Des initiatives similaires ont été lancées par des associations professionnelles comme le *World Wide Web Consortium* (W3C) ; cette dernière information est communiquée par les États-Unis, qui soulignent l'existence d'outils logiciels pour aider les entreprises à traduire leur politique de protection des données privées sous la forme d'une Plate-forme de préférences en matière de données privées (P3P) lisible par l'ordinateur et qui permet à l'entreprise d'inventorier tous les éléments de son site Web, afin d'évaluer et de limiter les risques en matière de données privées. En Allemagne, la loi d'application générale sur la protection des données privées comprend une disposition sur l'examen des pratiques de protection des données privées, dont la mise en œuvre sera réglée par des lois plus spécifiques.

L'Australie et les États-Unis indiquent que les pouvoirs publics encouragent les entreprises à analyser de leur propre initiative leurs pratiques en matière de protection des données privées. Dans le cas particulier des accords de *safe harbour* (ou sphère de sécurité) aux États-Unis, les participants doivent évaluer leurs propres pratiques ou cette évaluation doit être effectuée par un tiers. Aux Pays-Bas, l'autorité de protection des données a mis au point des outils d'audit en coopération avec des organismes privés (par

exemple une méthode d'autoévaluation et un protocole pour les audits de protection des données privées). Au Mexique et en Suède, les entreprises se soumettent volontairement à cette autoévaluation. La plupart des pays indiquent que les résultats de ces autoévaluations ne sont généralement pas accessibles au public. Toutefois, aux États-Unis une partie des entreprises (mais pas toutes) publient leurs autoévaluations. La République slovaque est le seul pays où l'autoévaluation est imposée par la loi.

Agences gouvernementales et organismes de surveillance émanant du secteur privé

Dans les pays dotés d'agences gouvernementales de protection des données, ces autorités ont compétence pour veiller au respect des normes. D'autres agences gouvernementales peuvent aussi surveiller la conformité aux normes dans des secteurs spécifiques (par exemple, l'Autorité finnoise de régulation des télécommunications, ainsi que les opérateurs de télécommunications, les équipementiers de télécommunications et les associations d'utilisateurs travaillent pour la protection des données privées et la sécurité de l'information dans les télécommunications). Dans les pays où il existe des systèmes de mise en conformité émanant du secteur privé (États-Unis, Japon), les entités qui administrent ces systèmes veillent en même temps au respect des normes, en association avec les agences gouvernementales compétentes.

L'organisation et les pouvoirs des organismes de régulation gouvernementaux sont déterminés par la législation. Les organismes de surveillance du secteur privé sont généralement mis sur pied à la suite d'accords procédant des participants au système. Les organismes gouvernementaux ont les compétences de surveillance qui leur sont octroyées par la loi, à savoir généralement celles de réaliser des examens, d'émettre des avertissements et de rendre compte des infractions à l'autorité compétente (comme c'est le cas en France). Les entités émanant du secteur privé ont souvent des compétences comparables et peuvent aller jusqu'à répondre aux réclamations et demandes de renseignements et à exclure les acteurs qui contreviennent au système, mais sans l'arsenal complet des sanctions dont disposent les organismes gouvernementaux.

Responsables internes de la confidentialité des données privées dans l'entreprise

D'après les réponses, les sociétés sont de plus en plus nombreuses à nommer un responsable interne de la confidentialité des données ; dans certains pays, c'est une obligation légale. L'USCIB et le gouvernement des États-Unis notent que les organes d'autorégulation peuvent dispenser des conseils sur les politiques et les pratiques, que plus de 500 entreprises se sont dotées d'un responsable principal de la confidentialité des données *(chief privacy officer)* chargé de veiller à ce que l'entreprise se conforme à la législation existante et applique les pratiques exemplaires. Ils signalent également qu'il existe maintenant des organisations qui chapeautent les travaux des entreprises dans l'établissement de pratiques et de procédures en la matière. Les États-Unis ajoutent que les entités visées par la loi sur les soins de santé *(Health Insurance Portability and Accountability Act)*, c'est-à-dire les caisses d'assurance maladie, les professions de santé et les organismes de remboursement, seront tenues par la loi de nommer un responsable de la sécurité à partir de l'entrée en vigueur de la loi (avril 2003). Par ailleurs, en Corée, les sociétés doivent nommer un responsable de la confidentialité des données chargé de protéger les données et de traiter les réclamations des personnes concernées. En République slovaque, si un maître de fichier emploie plus de cinq personnes, il doit nommer un ou plusieurs responsables pour veiller à la conformité avec les dispositions législatives en matière de traitement des données nominatives. Enfin, en Allemagne, les entités publiques et privées qui comptent plus de quatre employés doivent nommer un responsable de la protection des données. Pratiquement aucun autre répondant ne parle d'une obligation légale pour les entreprises de nommer un responsable de la confidentialité des données privées chargé de veiller au respect des règles. En Finlande, toutefois, un médiateur (*ombudsman*) de la protection des données a recommandé aux entreprises de désigner un responsable de la confidentialité, de même que plusieurs programmes

d'autorégulation au Japon et les autorités de protection des données de Norvège, du Royaume-Uni et de Suisse. La législation de certains pays membres (notamment l'Allemagne, les Pays-Bas et la Suède) dispense de certaines obligations légales (comme la déclaration des traitements de données à l'autorité de protection des données) les entreprises qui se dotent d'un responsable de la confidentialité des données privées.

Déclaration

La déclaration des traitements de données à une entité de supervision est obligatoire en Autriche, Belgique, aux États-Unis, Finlande, France, Italie, Norvège, République slovaque, République tchèque, Suède et Suisse. Toutefois, même dans ces pays, il existe des exceptions ou bien la déclaration n'est obligatoire que dans certaines situations. En Suède, par exemple, elle est facultative si un responsable de la confidentialité des données à caractère personnel a été nommé ou si le traitement a reçu le consentement de l'individu. De même au Japon, la déclaration des traitements à un service de supervision est obligatoire dans le cadre du programme de sceau de confidentialité TRUSTe. Au Mexique, les banques sont tenues de déclarer les traitements de données dans certaines circonstances.

Solutions technologiques

La plupart des répondants indiquent que des solutions technologiques de protection des données privées ne sont que peu employées, même si quelques pays membres (États-Unis, Japon, Royaume-Uni) déclarent que l'utilisation de normes techniques (comme P3P) pour assurer le respect des règles tend à se diffuser. Au Royaume-Uni, le Commissaire à la sécurité des données *(Information Commissioner)* préconise l'utilisation de technologies protectrices, et aux États-Unis on trouve de nombreux outils sur l'Internet (notamment P3P) mais on ne sait pas quelle proportion d'entreprises ou de consommateurs les utilisent. En Allemagne, le ministère de l'Économie et de la Technologie a lancé un programme pour encourager l'anonymat dans l'utilisation des technologies en ligne. Les Pays-Bas précisent que le gouvernement néerlandais s'est engagé à utiliser des technologies de protection des données dans les nouveaux systèmes publics de traitement des données. Ces initiatives sont toutefois des exceptions. Par ailleurs, l'utilisation d'outils technologiques de protection des données privées est évoquée dans le contexte de la sécurité. En Autriche et dans d'autres pays, l'utilisation de logiciels pare-feu, d'anti-virus et d'autres dispositifs de sécurité est généralisée et la loi exige que des mesures de protection pour les données soit en place mais ne précise pas quelles techniques doivent être employées. La Finlande indique que la situation est très variable selon les entreprises, selon la taille et le secteur d'activité. Le Japon indique que le *Secure Socket Layer* (SSL) et d'autres technologies de cryptage sont utilisées pour protéger certaines informations sensibles comme les numéros de carte de crédit ; c'est aussi le cas en Turquie.

Mise en œuvre

Autorités publiques

Dans tous les pays membres il existe au moins une autorité publique qui a compétence pour sanctionner les manquements aux normes de respect des données privées (tribunaux, police, agences de défense des consommateurs, agences de protection des données, autorités de régulation des télécommunications, autorités de concurrence, notamment). L'Italie indique que la loi permet aux personnes concernées de se retourner vers les maîtres de fichiers pour faire valoir leurs droits en cas de litige. Les États-Unis, le Japon et le Royaume-Uni notent que les individus doivent aussi pouvoir recourir à un dispositif d'autorégulation dans les cas où il en existe un qui est applicable.

La plupart des répondants indiquent qu'il est possible d'obtenir une réparation judiciaire ou administrative en portant l'affaire auprès des tribunaux ou d'instances gouvernementales, notamment des dommages et intérêts, un jugement d'injonction, l'effacement des données ou le blocage des traitements. L'Autriche note que la plupart des plaintes portées contre des entités privées doivent l'être devant les tribunaux, mais que de nombreuses plaintes concernant des questions de protection des données privées peuvent être résolues par le biais d'autres instruments judiciaires (droit des média, droit de la concurrence, droit des télécommunications et lois contre la diffamation et la calomnie). Les États-Unis précisent que la *Federal Trade Commission* (FTC) peut intenter des poursuites administratives ou judiciaires contre les entreprises qui diffusent des informations mensongères sur leurs pratiques internes en matière de protection des données privées, et qu'elle peut obtenir un jugement d'injonction ou le versement d'indemnités aux consommateurs lésés. La quasi-totalité des répondants indiquent que des amendes pénales ou administratives sont possibles. Les entités qui ont compétence pour imposer ces amendes sont notamment : les autorités pénales, les autorités de protection des données et les autorités de protection des consommateurs. La plupart des répondants, à l'exception de l'Australie et de la Belgique, indiquent que les sanctions pénales sont possibles – amendes, voire emprisonnement. Les États-Unis notent que cette compétence est très étroitement encadrée. Tous les répondants indiquent en outre que des jugements d'injonction peuvent être prononcés par les tribunaux ou par les autorités de protection des données, ou par les deux. En Belgique et en France, les autorités de protection des données ne peuvent pas imposer elles-mêmes le jugement d'injonction, mais elles peuvent saisir un tribunal à cette fin.

Entités du secteur privé

S'agissant des sanctions que les entités peuvent imposer en cas de violation, les répondants citent le retrait des sceaux et marques de confiance, la radiation des instances d'autorégulation et l'inscription en liste noire. Plusieurs (comme la Finlande, la Norvège et la République slovaque) notent que dans leur pays un organisme privé ne peut pas lui-même imposer une amende ou prendre une mesure punitive, mais qu'il peut porter une affaire devant un tribunal ou une autorité de protection des données. L'USCIB note que la dégradation de l'image publique d'une entreprise sur le marché est très pénalisante, et qu'aux États-Unis, les affaires de violation présumée du respect des données privées sont généralement traitées rapidement par les organisations, soucieuses qu'elles sont de préserver leur réputation. Le Japon indique qu'une instance d'autorégulation peut presser les entreprises qui lui appartiennent de prendre certaines mesures ; des sanctions, comme la radiation, peuvent être invoquées pour donner plus de poids à ces injonctions.

Traitement des plaintes

Il existe un large éventail de procédures utilisées pour traiter les plaintes pour violation de la confidentialité de données privées. Dans la plupart des pays membres, les plaintes sont déposées auprès des autorités de protection des données ou de protection des consommateurs. Celles-ci peuvent enquêter sur le dossier et prendre les mesures nécessaires, qui peuvent aller jusqu'à l'imposition de pénalités ou le renvoi devant les tribunaux ou les autorités pénales. Dans certains pays (l'Italie notamment), c'est la personne concernée qui doit d'abord saisir le maître de fichier avant de réclamer des réparations auprès des autorités de protection des données, alors que dans d'autres (comme la Suède), la personne concernée peut, soit s'adresser directement aux autorités, soit saisir le maître de fichier. Comme le souligne le Japon, les organismes d'autorégulation ont chacun leurs propres procédures pour traiter les plaintes.

Dépôt de plainte en ligne et MARC

Le dépôt de plaintes en ligne est possible dans plusieurs pays membres (citons l'Allemagne, l'Australie, l'Autriche, les États-Unis, la France, le Japon et la Suède). La Norvège indique que, si le dépôt

de plaintes en ligne n'est pas prévu formellement, il est utilisé dans la pratique (c'est-à-dire que les personnes concernées envoient fréquemment des plaintes ou des demandes de renseignements par courrier électronique aux autorités de protection des données). Le Royaume-Uni travaille à l'élaboration d'un système de dépôt des plaintes en ligne. Le Mexique précise que l'Agence fédérale de protection des consommateurs (Profeco) a pris part à un projet international conduit dans le cadre du Réseau international de contrôle du commerce (RICC) qui a conduit à l'établissement d'un site Web centralisant les plaintes concernant le commerce électronique transfrontière[8]. Aux États-Unis, la FTC gère le site du projet RICC, outre son propre site Web[9] permettant aux consommateurs de déposer des plaintes concernant les données privées sur Internet, notamment celles qui concernent les affirmations mensongères et les transactions de commerce électronique.

Les modes alternatifs de règlement des conflits (MARC), comme l'arbitrage et la médiation, sont utilisés pour les litiges liés à la protection des données dans une minorité de pays (Autriche, Corée et États-Unis). La France indique que la Commission européenne travaille à l'élaboration de plusieurs systèmes de ce type. L'Italie note que des mécanismes de MARC sont utilisés mais qu'il n'en existe pas qui soient prévus spécialement pour les litiges concernant l'utilisation des données privées. Le Japon est en train de mettre sur pied des systèmes de MARC. En Allemagne, de tels mécanismes sont proposés par quelques organismes de marques de confiance.

Audit

Seuls un petit nombre de pays indiquent que l'audit des pratiques en matière de protection des données privées est utilisé comme méthode de contrôle. En Finlande, le Médiateur (*ombudsman*) de protection des données a compétence pour auditer les fichiers de données à caractère personnel et l'Autorité finnoise de régulation des télécommunications peut auditer les activités des opérateurs de télécommunications. En France, la Commission nationale de l'informatique et des libertés (CNIL) a recours à des enquêtes en ligne pour inventorier les pratiques des sites Web. Aux États-Unis et au Japon, des audits sont pratiqués par des organismes d'autorégulation ; au Mexique, ils sont volontaires. L'audit peut également constituer une forme de mécanisme de contrôle à la disposition d'agences gouvernementales, comme c'est le cas aux États-Unis et en Suède. En Allemagne, quelques agences locales de protection des données conduisent des audits de sites Web à l'aide d'outils logiciels. De nombreux répondants indiquent que la sécurité des systèmes d'information et des réseaux informatiques fait souvent l'objet d'audits de sécurité.

Sensibilisation du public

Méthodes

La plupart des pays indiquent que des campagnes d'initiative publique ou privée ont été organisées pour sensibiliser le public sur ses droits en matière de protection des données. Parmi les méthodes utilisées on peut citer : les discours et les réunions, les interviews média, la diffusion de publications, l'information dispensée sur les sites Web des agences de protection des données privées[10], la publication du rapport annuel de ces agences, la création par les entreprises de kits de protection des données privées et les dispositifs des organismes d'autorégulation indiquant aux utilisateurs comment limiter la circulation d'informations nominatives les concernant, leur expliquant leurs options quant à l'utilisation et la circulation de ces informations, et précisant dans quelles conditions ils peuvent y accéder.

Politiques en matière de protection des données privées

Aucun répondant ne fait état de dispositions législatives faisant expressément obligation aux sites Web de publier leurs pratiques en matière de protection des données. Toutefois, dans de nombreux pays membres, les maîtres de fichiers (notamment les opérateurs de sites Web) ont l'obligation légale d'informer la personne du traitement de données la concernant (y compris certains aspects comme les droits d'accès, etc.) et cette obligation peut être satisfaite grâce à une politique en matière de protection des données. De nombreux dispositifs émanant des autorités ou du secteur privé encouragent aussi les entreprises à publier en ligne leurs pratiques de protection des données privées. Dans certains cas, ce document peut contenir des mentions obligatoires, comme l'identité du maître de fichier et la finalité du traitement. Il ressort de plusieurs réponses qu'un nombre croissant de sites Web communiquent en ligne sur leur politique en matière de protection des données privées.

Personnes à contacter

Dans deux pays seulement, la Belgique et la République slovaque, la législation impose la désignation d'une personne à contacter pour obtenir des informations sur les pratiques en matière de protection des données privées, ou à qui adresser les réclamations ou les questions. Toutefois, la plupart des pays indiquent qu'il existe des incitations à cette désignation. En France par exemple, la loi encourage les entreprises à nommer une personne à contacter en matière de droits d'accès et de rectification, puisque les déclarations à la CNIL doivent préciser le nom du service de l'entreprise à qui doivent être adressées les demandes d'accès et de rectification des données à caractère personnel.

Publicité sur les violations

Les violations des normes de protection des données font-elles l'objet d'une publicité, et si oui, laquelle et par qui ? Les réponses varient considérablement sur ce point. Quelques répondants (le Mexique et la Turquie notamment) déclarent sans ambiguïté que les violations ne font l'objet d'aucune publicité, à la différence des pays (comme l'Italie) où cette publicité existe. La plupart des pays membres indiquent qu'il existe des possibilités de publicité, mais qu'elles sont restreintes. Par exemple en Autriche, les décisions sont publiées en ligne, mais sans référence nominative ; en Belgique, seules les décisions ayant des répercussions importantes sont publiées par voie de communiqués de presse; en République tchèque, les autorités de protection des données ne rendent compte des décisions qu'en termes génériques par le biais de leurs rapports annuels, mais sans reproduire le texte des décisions ; en République slovaque, seules les infractions les plus graves sont publiées. Aux États-Unis, les enquêtes de la FTC sur les violations présumées de la confidentialité des données ne sont pas publiques, mais lorsqu'une action administrative ou judiciaire est intentée, elle est publiée sur le site de la FTC. La *Direct Marketing Association* aux États-Unis signale également que le *Safe Harbor Enforcement Program Contract* comprend des dispositions permettant à la DMA de publier des communiqués de presse faisant état de certaines décisions. Plusieurs répondants indiquent que la publicité des violations, qu'elle soit faite par des instances gouvernementales ou dans le cadre de systèmes disciplinaires d'autorégulation, peut être un moyen très efficace de mise en œuvre ; par ailleurs, la France note que la publicité sur les violations de données privées peut avoir des retombées judiciaires (diffamation et autres poursuites civiles), et que la prudence est de mise pour traiter chaque affaire. Le Commissaire à la sécurité des données du Royaume-Uni a récemment effectué une étude sur le respect des normes en matière de données privées sur les sites Web ; ce travail est publié sur le site Web du Commissariat à la sécurité des données[11].

II. Analyse

Les lignes directrices de l'OCDE régissant la protection des données privées

Les lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel comprennent deux types de dispositions concernant le respect et la mise en œuvre : *i)* les dispositions qui énoncent des principes généraux applicables au traitement des données (limitation de la collecte, qualité de l'information, limitation de l'utilisation, etc.), et *ii)* les dispositions concernant les intérêts des individus en relation avec leurs données à caractère personnel (principe de la participation individuelle, principe de la responsabilité, mise en œuvre à l'échelon national). Le premier ensemble de dispositions, bien que présenté sous forme de conditions pour le traitement des données à caractère personnel, touche indirectement au respect et à la mise en œuvre, puisqu'il comprend les pratiques recommandées aux organisations qui traitent des données à caractère personnel. Le deuxième ensemble de dispositions concerne plus directement les recommandations sur les droits dont devraient bénéficier les individus sur les données qui les concernent (Partie 2. Principes fondamentaux applicables au plan national, paragraphe 13) ainsi que les recommandations destinées aux pays membres de prévoir des mécanismes de responsabilité (Partie deux. Principes fondamentaux applicables au plan national, paragraphe 14) ; de mettre en œuvre ces principes en s'efforçant d'adopter des législations nationales appropriées ; d'encourager et de soutenir l'autorégulation, quelle prenne la forme de codes de conduite ou d'autres formes ; de prévoir des moyens raisonnables permettant aux individus de faire valoir leurs droits ; de prévoir des sanctions et des voies de recours adéquates en cas de non respect des mesures qui traduisent les principes ; et de veiller à ce que les personnes concernées ne soient pas victimes de discrimination (Partie 4, Mise en œuvre des principes à l'échelon national, paragraphe 19).

Les Lignes directrices de 1980 disposent ainsi que les États devraient reconnaître aux individus certains droits sur les données à caractère personnel les concernant ; que le maître du fichier devrait être responsable du respect des mesures qui constituent la traduction de ces droits ; que les pays membres devraient mettre en œuvre certaines procédures juridiques, administratives ou autres pour protéger la vie privée et les libertés individuelles en liaison avec les données nominatives. Dans le même temps, les Lignes directrices ne présentent pas en détail les mécanismes par lesquels cette protection doit être assurée; elles ne font que suggérer des méthodes auxquelles peuvent recourir les pays membres pour mettre en œuvre les principes de l'OCDE en matière de respect des données privées (voir paragraphe 19 précité). D'après les Lignes directrices, le meilleur système pour assurer le respect et la mise en œuvre repose sur une combinaison de réglementation gouvernementale et d'autorégulation émanant du secteur privé.

L'évolution des cadres législatifs nationaux en matière de protection des données

A l'origine, s'agissant des données à caractère personnel, la plupart des pays membres se sont dotés de cadres juridiques qui visaient principalement, par des disciplines et des sanctions, à assurer un bon niveau de respect des normes et à protéger les droits des personnes. Ces cadres privilégiaient des mécanismes « traditionnels » de contrainte permettant aux individus de faire valoir leurs droits: plaintes auprès des autorités de protection des données ou d'autres organes gouvernementaux, actions en justice ; il s'agissait également d'assurer l'existence de sanctions adéquates en cas d'infraction à la législation.

Toutefois, un certain nombre d'évolutions intervenues depuis l'apparition de la législation et des mécanismes de régulation en matière de protection des données sont venues compliquer le respect des règles de protection des données et leur sanction :

- La mondialisation de l'économie s'est nettement accentuée depuis 20 ou 30 ans et il est devenu banal que des individus d'un pays effectuent des transactions avec des entités situées à l'étranger par le biais des réseaux de télécommunications.

- L'utilisation d'équipements informatiques pour traiter les données à caractère personnel a progressé à un rythme exponentiel et dans des proportions inimaginables il y a encore quelques années.
- Les dispositifs en ligne comme les portails, les places de marché et les communautés se sont multipliés ; tout en restant soumis au droit existant en matière de données privées, ces organisations fonctionnent essentiellement suivant des règles qu'elles ont édictées elles-mêmes et des conditions convenues avec les utilisateurs.
- Le concept de technologies protectrices de la vie privée (PET) s'est développé ; il s'agit d'intervenir avant qu'il y ait infraction aux normes de protection des données privées.
- Le nombre de litiges portés devant les tribunaux à la suite d'interactions transfrontières en ligne n'a cessé d'augmenter[12].

Comme en témoignent les réponses au questionnaire, ces évolutions ont fondamentalement modifié le paysage juridique en matière de vie privée, tant au niveau du respect qu'à celui de la mise en œuvre. Le principe suivant lequel il appartient à l'État de sanctionner les violations de la loi demeure, certes, le fondement de la confiance des utilisateurs individuels dans le domaine de la protection des données privées, mais les mécanismes traditionnels (amendes, enquêtes des autorités de protection des données, actions en justice) sont de plus en plus souvent relayés par des moyens alternatifs et complémentaires pour assurer le respect et la mise en œuvre en matière de protection des données privées.

Comme le démontrent les réponses au questionnaire, les pays de l'OCDE et les organismes du secteur privé élaborent des moyens alternatifs pour assurer le respect et la mise en œuvre du droit en matière de données privées, qui vont bien au-delà des règlements et des sanctions classiques des autorités publiques. Ces méthodes alternatives présentent un certain nombre de caractéristiques :

- Elles privilégient souvent les incitations et les sanctions reposant sur les mécanismes de marché pour pousser au respect des normes. Par exemple, de nombreux programmes de marque de confiance et de sceau de confidentialité ont été élaborés, qui imposent aux sites Web participants de se conformer à certaines pratiques en matière de confidentialité. En cas de manquement, le sceau ou la marque de confiance peut leur être retiré, accompagné d'une publicité négative. Ces dispositifs exercent une pression dissuasive sur les participants.
- Elles s'appuient souvent sur des moyens techniques pour assurer le respect des normes. Les pays membres comme les organismes privés encouragent les acteurs à utiliser des technologies protectrices des données privées (P3P, par exemple), à pratiquer des audits, et à appliquer d'autres mécanismes de ce type pour veiller à ce que les données à caractère personnel soient traitées en conformité avec les principes applicables en matière de confidentialité. En favorisant la discipline en amont, on limite le recours ultérieur aux sanctions.
- Les entreprises, sensibilisées aux avantages qu'elles peuvent retirer en termes commerciaux si elles protègent les données à caractère personnel de leurs clients, proposent pour cela un grand nombre d'instruments, de mécanismes et de systèmes de protection des données. Parmi ces dispositifs d'autorégulation on peut citer les programmes de marque de confiance, les sceaux, les PET, la nomination de responsables internes de la confidentialité, la publication en ligne de politiques de la vie privée, etc.
- Une démarche très prometteuse consiste à transposer les mécanismes existants de respect et de mise en œuvre des normes en matière de données privées dans l'environnement en ligne. Par exemple, des pays membres et des entreprises ont donné aux individus la possibilité déposer une plainte en ligne, et plusieurs MARC (mécanismes alternatifs de règlement des conflits) destinés aux litiges en matière de confidentialité sont à l'étude.

- La sécurité est une composante de plus en plus essentielle de la confidentialité des données. Il n'est donc pas surprenant que des gouvernements et des entités aient œuvré pour la diffusion de normes techniques, d'audits, de politiques de sécurité et d'autres mécanismes afin d'assurer la sécurité des traitements de données en ligne.

Ces évolutions ont profondément bouleversé le paysage de la protection de la vie privée, tant sous l'angle du respect que sous celui des sanctions. Ces aspects, jusqu'ici perçus dans une perspective législative ou réglementaire, apparaissent désormais de manière plus globale : l'action de régulation exercée par les autorités publiques ne représente plus qu'un élément de la politique visant à assurer le respect et la mise en œuvre des normes ; elle doit être couplée à des mécanismes techniques, organisationnels et d'autorégulation afin d'atteindre une efficacité maximum dans un environnement en ligne mondialisé. De plus, il est essentiel d'avoir une vision mondiale et non plus nationale de la protection des données à caractère personnel pour faciliter les recours en cas de violation transfrontière. Il est moins onéreux de veiller au respect des normes avant les faits, et cela impose moins de démarches aux personnes concernées que si elles doivent faire valoir leurs droits devant les tribunaux ou par d'autres moyens. Dans cette optique, un grand nombre d'initiatives ont été lancées, et tout porte à croire que cette approche devrait continuer de se diffuser rapidement dans les années qui viennent.

Autres mesures

Dans le même temps, les efforts des pays membres doivent être renforcés afin d'encourager l'usage de mécanismes alternatifs et d'autorégulation pour favoriser le respect et la mise en œuvre des normes en matière de données à caractère personnel, en particulier dans les domaines suivants :

- La coordination internationale et transfrontière des mécanismes et de la mise en œuvre des normes est essentielle, tant pour protéger les données des personnes que pour éviter que les maîtres de fichiers ne soient soumis à des normes différentes pour une même pratique. Les pays membres doivent donc faire tout leur possible pour coordonner leurs efforts en matière de respect et de mise en œuvre afin de protéger les personnes concernées tout en minimisant les procédures excessivement lourdes pour les maîtres de fichiers, et pour prévoir des solutions suffisamment souples pour assurer une protection efficace sans pour autant entraver les flux de données, comme le recommandent les Lignes directrices de l'OCDE (voir par exemple le paragraphe 7 de l'Exposé des motifs des Lignes directrices). Actuellement, ces mécanismes sont trop souvent d'application nationale ou régionale et non mondiale. Il faut que les pays membres collaborent pour établir une coopération internationale en matière de respect des normes et de sanctions. En particulier, ils doivent prendre des mesures notamment pour permettre un meilleur partage des ressources consacrées au traitement des plaintes et pour sensibiliser les particuliers et les entreprises aux réglementations et aux pratiques exemplaires, et pour soutenir l'émergence d'un marché du MARC en ligne et des PET. Autre objectif, les pays membres doivent renforcer les sanctions contre les sociétés qui font des déclarations ou des promesses mensongères quant à leurs pratiques de protection, particulièrement lorsque ces déclarations peuvent avoir des conséquences de nature à porter préjudice aux clients.
- Les mesures visant à encourager la mise en œuvre de solutions techniques pour le respect et la mise en œuvre de la confidentialité (P3P, notamment) apparaissent insuffisantes : seul un petit nombre de pays mentionnent une activité dans ce domaine. Les pays membres doivent faire un travail de pédagogie et de sensibilisation à propos de ces solutions techniques, et encourager leur développement et leur utilisation. Il faut particulièrement promouvoir l'utilisation des PET pour améliorer la protection des personnes concernées.
- Actuellement, l'utilisation de certains mécanismes d'autorégulation particulièrement prometteurs pour la protection de la confidentialité en ligne semble assez parcellaire, et se limite à un petit

nombre de pays. Par exemple, il ressort des réponses que dans certains pays, on n'utilise pas aussi souvent qu'on le pourrait des mesures visant à encourager les entreprises à pratiquer des autoévaluations de leurs pratiques en matière de confidentialité des données privées.

- Les pays membres devraient être plus nombreux à encourager la nomination de responsables de la confidentialité des données. Ils pourraient par exemple créer pour ces acteurs un statut juridique et/ou accorder des avantages juridiques aux entreprises concernées. Actuellement, dans quelques pays, la nomination d'un responsable de la confidentialité pour superviser les traitements de données est prévue par la loi alors que dans d'autres, les sociétés le font à titre purement volontaire ou dans le cadre de dispositifs d'autorégulation.
- Les MARC en ligne, si leur élaboration suscite actuellement une intense réflexion, restent utilisés par trop peu de pays. Le développement des systèmes de MARC pourrait être déterminant pour améliorer la position juridique des personnes qui veulent faire valoir leurs droits, et il faut faire davantage dans ce sens. Il est particulièrement important que ces systèmes soient élaborés en tenant compte de la nature mondiale du commerce électronique : ils doivent fonctionner dans plusieurs langues et permettre de régler les litiges transfrontières.
- Étant donné la recrudescence probable des plaintes et le manque de ressource des États pour les traiter, les pays membres doivent privilégier les secteurs dans lesquels les utilisateurs subissent les plus grands préjudices en cas d'utilisation abusive des données les concernant.

Ainsi, on constate que les pays membres progressent vers un régime plus satisfaisant en matière de respect et de mise en œuvre des normes de protection des données privées en ligne, mais beaucoup reste à faire. L'essentiel pour les années à venir sera de rendre encore plus efficaces les voies classiques de régulation, tout en encourageant le développement des mécanismes d'autorégulation, car la combinaison de ces deux systèmes apparaît comme la meilleure protection des intérêts des individus et des maîtres de fichiers. De plus, il est essentiel que tous les mécanismes développés puissent être appliqués sur une base transfrontière.

NOTES

1. Directive 95/46/CE du Parlement européen et du Conseil 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 (1995), *Journal officiel des Communautés européennes* L281, p. 31.

2. La sphère de sécurité *(safe harbor)* est un système de protection des données privées relevant de l'autorégulation. Le 26 juillet 2000, la Communauté européenne a déclaré que les principes de la sphère de sécurité assurent une protection adéquate aux données transférées depuis l'UE vers les États-Unis. On trouvera une documentation complète sur cette notion à : www.export.gov/safeharbor/sh_overview.html

3. La Commission européenne a reconnu la validité des contrats types de transfert de données pour les transferts entre maîtres de fichiers [Décision de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (2001) JO L181/19] et entre maîtres de fichiers et responsables de traitement des données [Décision de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE (2002), *Journal officiel* L6/52].

4 . Parmi ces accords, on peut citer notamment la Convention pour la mise en place d'un Office européen de police (Convention Europol), la Convention sur l'emploi de l'informatique dans le domaine des douanes , et la Convention d'application de l'accord de Schengen relatif à la suppression graduelle des contrôles aux frontières communes (Convention de Schengen). De plus, l'accord de la ZEE (Zone économique européenne) entre l'UE et trois pays de l'AELE (Association européenne de libre échange) stipule que les instruments de protection des données en vigueur dans l'UE sont applicables dans les trois États de l'AELE parties à l'accord. L'AELE comprend l'Islande, le Liechtenstein, la Norvège et la Suisse.

5. La liste complète des membres du Conseil de l'Europe et la liste des États ayant ratifié la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel est consultable à : http://conventions.coe.int/Treaty/EN/cadreprincipal.htm. Cette convention a été ouverte à la signature le 28 janvier 1981. Pour le texte de la convention, voir www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/.

6. La version finale des dispositions a été remise à la Commission européenne le 9 août 2002 et se trouve à : www.iccwbo.org/home/electronic_commerce/word_documents/Final%20version%20July%202002%20Model%20contract%20clauses.pdf.

7. Conseil de l'Europe/Commission européenne/CII, Contrat-type du 2 novembre 1992 visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données et rapport explicatif.

8. Dix-sept pays membres font partie de ce projet. Voir www.econsumer.gov.

9. www.ftc.gov.

10. Pour le Royaume-Uni voir www.dataprotection.gov.uk/dpr/dpdoc.nsf.

11. Ce rapport peut être consulté à : www.dataprotection.gov.uk/dpr/dpdoc.nsf à la rubrique Guidance and Other Publications: Codes of Practice our Responses and Other Papers: Related Papers: UMIST UK Website Compliance Study.

12. Cette augmentation est indiquée par les statistiques du gouvernement sur le nombre de plaintes reçues sur le site www.econsumer.gov.

APPENDICE

QUESTIONNAIRE SUR LE RESPECT DES RÈGLES DE PROTECTION DE LA VIE PRIVÉE ET SUR LEUR MISE EN ŒUVRE DANS LE CONTEXTE DU COMMERCE ÉLECTRONIQUE ENTRE ENTREPRISES ET CONSOMMATEURS

1. Vos réponses devront :

- Porter sur les activités en ligne. Si vous faites référence à des éléments ne concernant pas spécifiquement les activités en ligne, veuillez indiquer de quelle manière ces informations s'appliquent dans l'environnement en ligne.
- Cibler le commerce électronique de détail B2C *(business-to-consumer)*. Les gouvernements pourront aussi, s'ils le souhaitent, ajouter des informations concernant le secteur public.
- Couvrir le champ le plus large. En particulier, vos réponses devront décrire non seulement les approches réglementaires, mais aussi les dispositifs d'autorèglementation comme la nomination de responsables de la protection de la vie privée, les sceaux de confidentialité, les procédures d'audit, les organisations professionnelles, les technologies (notamment les technologies protectrices de la vie privée), etc.
- Faire la distinction, le cas échéant, entre les approches réglementaires et non réglementaires en matière d'autorèglementation et de mise en œuvre, de manière générale et dans les différents secteurs. Veuillez également évoquer les dispositions légales et d'autorèglementation qui ne visent pas spécifiquement la protection de la vie privée, mais qui peuvent toutefois avoir un impact sur elle.
- Signaler le cas échéant les différences entre les mécanismes lorsqu'ils sont appliqués dans un cadre national ou international. Décrire les dispositifs nationaux, en insistant particulièrement sur leur application au niveau transfrontière.
- Indiquer s'il existe des mécanismes ou des initiatives de coopération pour assurer le respect et la mise en œuvre de la protection de la vie privée au niveau mondial (cadre officiel bilatéral ou multilatéral, ou coopération transfrontière informelle).

Les termes « dispositions législatives », « non réglementaires » et « autorèglementation » doivent s'entendre au sens le plus générique, général et large qui soit.

2. Normes et instruments

Ces questions ont pour but d'identifier les normes et points de référence utilisés pour le respect et la mise en œuvre des principes de protection de la vie privée au niveau national. Veuillez indiquer les références de ces normes et instruments, ainsi que les dispositions visant les questions transfrontières et internationales.

Indiquez les éléments qui pourraient servir de fondement juridique à des droits et à des obligations en matière de protection de la vie privée :

2.1 Existe-t-il une ou plusieurs lois de protection de la vie privée et des données à caractère personnel ? Dans l'affirmative, est-ce une loi d'application générale ou une série de lois sectorielles, ou les deux ?

2.2 Existe-t-il d'autres formes de réglementation dans ce domaine (décrets, ordonnances, règlements administratifs, jurisprudence, etc.) ?

2.3 Votre pays est-il partie à des accords de droit public ou à d'autres instruments dans le domaine de la protection de la vie privée (*Safe Harbour*, par exemple) ?

2.4 Votre pays a-t-il mis en œuvre d'autres accords ou instruments de droit privé pouvant servir de fondement à la protection des données (ex : clauses contractuelles modèles pour le transfert des données) ?

2.5* Existe-t-il des codes de conduite professionnels approuvés par une entité gouvernementale ?

2.6* Existe-t-il des codes de conduite sectoriels privés, des recueils de pratiques exemplaires, des programmes de sceau de confidentialité ou de marques de confiance qui soient entérinés par une association professionnelle, ou largement reconnus par l'ensemble des entreprises ou par un secteur en particulier ?

2.7* Existe-t-il une réglementation gouvernementale ou des pratiques du secteur privé imposant aux sites Web d'appliquer des politiques, des règles ou des mesures techniques de protection des données à caractère personnel des visiteurs contre les accès non autorisés, l'utilisation ou la divulgation abusives de ces données, etc. ?

3. Respect des règles

Veuillez expliquer comment le respect des normes identifiées ci-dessus est assuré pour ce qui est de l'activité en ligne, dans un cadre national et dans un cadre transfrontières.

3.1* Où les compagnies obtiennent-elles des informations et des conseils afin d'assurer le respect des normes identifiées ci-dessus ? Ont-elles, par exemple, recours aux conseils d'un juriste (extérieur ou interne à la société), utilisent-elles des responsables du respect de la vie privée en interne (pour obéir à des obligations légales ou parce que c'est une pratique établie), s'adressent-elles à des consultants, à des agences de protection des données ou des consommateurs ?

3.2* Existe-t-il des procédures administratives, des examens fondés sur les pratiques exemplaires, des outils logiciels (utilisés pour la protection de la vie privée elle-même ou pour l'audit des pratiques s'y rapportant), ou d'autres moyens pour examiner les pratiques suivies par les entreprises qui exercent des activités en ligne ?

3.3* Existe-t-il des organismes de surveillance compétents pour vérifier le respect des normes citées ci-dessus ? S'agit-il d'agences gouvernementales, d'autorités indépendantes de protection des données ou d'organismes relevant du secteur privé ?

3.4* Comment ces organismes de surveillance sont-ils mis sur pied, et de quels pouvoirs disposent-ils ?

3.5* Les compagnies réalisent-elles de leur propre initiative une évaluation de leurs pratiques en matière de vie privée ? Dans l'affirmative, ces évaluations sont-elles accessibles au public ?

3.6* Les compagnies sont-elles incitées ou obligées à nommer un responsable de la protection de la vie privée chargé de veiller à son respect ?

3.7 Les compagnies sont-elles tenues de déclarer leurs traitements de données à un organisme de surveillance ?

3.8* Dans quelle mesure des solutions technologiques de protection de la vie privée sont-elles appliquées dans votre pays ?

3.9* Existe-t-il des procédures ou des processus visant à assurer le respect de la vie privée autres que ceux qui sont cités ci-dessus ?

4. Mise en œuvre

Veuillez expliquer comment les normes citées ci-dessus sont appliquées ?

4.1* A quelles organisations, entités ou personnes, les parties ou personnes concernées par le traitement de leurs donnés peuvent-elles s'adresser pour obtenir la mise en œuvre des normes ?

4.2 Quelles voies de recours existe-t-il pour les victimes, et comment les responsables de traitements qui transgressent les normes de respect de la vie privée peuvent-il être contraints à s'y conformer ?

4.3* Quels types d'actions les organisations professionnelles du secteur privé prennent-elles pour sanctionner les violations - par exemple retrait du sceau ou de l'indicateur de confiance, inscription de l'entreprise en liste noire ou action en justice ?

4.4 Existe-t-il des amendes administratives au pénales pour sanctionner les violations, et qui est habilité à requérir ces amendes ?

4.5 Un tribunal peut-il infliger d'autres peines, notamment des peines de prison ?

4.6 Les victimes peuvent-elles obtenir des dommages et intérêts en réparation du préjudice subi en cas de violation ?

4.7* Un organisme de surveillance (du secteur privé ou du secteur public), une autorité ou un tribunal peuvent-ils imposer l'exécution d'un droit, par exemple, exiger qu'il soit donné accès aux données à caractère personnel ou interdire un transfert de données ?

4.8* Quels types de procédures existent pour traiter les plaintes ?

4.9* Est-il possible de déposer des plaintes en ligne, ou y a-t-il d'autres possibilités d'utiliser des technologies Internet pour la résolution des litiges ?

4.10* Existe-t-il des mécanismes de résolution des litiges, comme les modes alternatifs de résolution des conflits (MARC), qu'ils relèvent du secteur privé ou du secteur public, afin de régler les litiges concernant le respect de la vie privée ?

4.11* L'audit des pratiques en matière de vie privée est-il utilisé comme méthode de mise en œuvre (ou mesure coercitive)? Dans l'affirmative, ces audits sont-ils volontaires, ou existe-t-il une obligation à faire l'objet d'un audit ? Noter que le terme « audit » doit ici être pris dans son sens le plus large, incluant l'analyse des pratiques par les professionnels, mais aussi l'audit des pratiques en ligne à l'aide d'outils logiciels (notamment les robots logiciels qui évaluent les pratiques du site ou pour repérer les endroits où est affiché un sceau ou un indicateur de confidentialité).

4.12* Des normes techniques sont-elles appliquées pour assurer la sécurité (P3P par exemple) ? Existe-t-il des incitations réglementaires à utiliser ces normes ?

5. Sensibilisation du public

Veuillez expliquer de quelle manière le public est, pour ce qui concerne l'environnement en ligne, informé de ses droits en matière de vie privée et des violations dans ce domaine.

5.1* Les compagnies sont-elles encouragées à ou obligées de faire figurer sur leur site une déclaration de politique de protection de la vie privée, ou d'indiquer la possibilité d'en référer à un organisme de surveillance sur ces questions, ou les deux ?

5.2* Les compagnies sont-elles encouragées à désigner une personne, comme point de contact, pour fournir des informations sur les pratiques de leur compagnie en matière de vie privée, recevoir des réclamations ou répondre à des questions ?

5.3* Les violations des normes de vie privée font-elles l'objet d'une publicité, et dans l'affirmative, laquelle (publication des informations sur l'Internet, publicité dans la presse par exemple) et par qui ?

5.4* Existe-t-il des campagnes de sensibilisation du public sur ses droits en matière de vie privée, qu'elles soient d'initiative publique ou privée ? Par quelle voie sont-elles menées ? S'agit-il de campagnes spécifiques ou d'activités continues et régulières ?

Chapitre 12

INVENTAIRE DES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE

Ce chapitre présente un inventaire des technologies protectrices de la vie privée (TPVP), examine les méthodes de collecte de données, analyse les différents types de technologies protectrices de la vie privée et formule des recommandations à l'intention du secteur privé pour stimuler le développement et l'utilisation de ces technologies.

Chapitre 12

INVENTAIRE DES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE

Introduction

La technologie peut grandement contribuer au renforcement de la protection de la vie privée dans le cyberespace. Inspiré des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (OCDE, 1980), le présent document a pour but d'analyser la disponibilité et la diversité des technologies protectrices de la vie privée, d'examiner les facteurs qui ont une incidence sur l'adoption de ces technologies, d'analyser la relation entre technologie et vie privée, et de servir de point de départ aux responsables de l'action gouvernementale pour leur réflexion sur l'utilisation et le déploiement de ces technologies.

Les technologies protectrices de la vie privée recouvrent des moyens très divers. Que ce soit en assurant l'anonymat ou en permettant à l'internaute de choisir s'il veut divulguer ou non des renseignements personnels le concernant, quand il veut le faire et dans quelles conditions, ces technologies aident à faire des choix éclairés en matière de protection de la vie privée.

Elles permettent d'autonomiser les internautes/consommateurs qui souhaitent contrôler la divulgation, l'utilisation et la diffusion dans le cyberespace des informations personnelles les concernant. Les technologies protectrices de la vie privée peuvent également aider les entreprises et les organisations à appliquer leurs propres politiques et pratiques en matière de protection de la vie privée. Compte tenu des préoccupations que cette question suscite chez les consommateurs, ces technologies de la confidentialité ont un rôle décisif à jouer dans la gestion des flux de renseignements à caractère personnel sur les réseaux publics mondiaux.

Le présent document examine les méthodes de collecte de données ainsi que les différents types de technologies protectrices de la vie privée et formule des recommandations pour en encourager une plus large utilisation. Il aborde aussi brièvement les technologies de la sécurité, dont beaucoup ont été à l'origine conçues pour préserver la confidentialité de l'information, mais peuvent également contribuer de façon plus générale à renforcer la protection de la vie privée. Par ailleurs, de nombreuses technologies qui améliorent la sécurité – comme les signatures numériques ou les technologies d'authentification – peuvent renforcer la protection de la vie privée dans les communications ou les transactions en ligne ou assurer l'intégrité de ces dernières, mais du fait qu'elles ont pour but de vérifier l'identité, elles sont susceptibles de limiter l'anonymat possible dans le cyberespace.

Étant donné la très grande diversité des technologies et des usages qu'on peut en faire, il est essentiel de bien définir le contexte dans lequel une technologie donnée sera utilisée. Les finalités de différents produits, technologies ou fonctions pourront varier selon les préférences de l'utilisateur et la mise en œuvre de l'option retenue. Il importe donc d'avoir présent à l'esprit que les consommateurs et les décideurs devront être sensibilisés à cet état de choses et comprendre les différentes façons d'utiliser les diverses technologies en fonction des objectifs visés.

Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (OCDE, 1980)

La rapide expansion des réseaux mondiaux interconnectés et la circulation de plus en plus dense de données à caractère personnel à travers les frontières nationales ont sensibilisé les responsables de l'action gouvernementale, les consommateurs et les entreprises à la question de la protection de la vie privée. Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ont été adoptées par l'Organisation de coopération et de développement économiques à une autre époque de développement et d'expansion technologiques mais elles n'ont rien perdu de leur pertinence et de leur actualité. En 1980, l'OCDE s'intéressait principalement à l'accroissement du traitement de données à caractère personnel transmises à travers les frontières nationales par de grandes entreprises et par des sociétés de traitement de données. Aujourd'hui, l'Organisation se penche sur la mise en commun et la diffusion de ces données à travers les frontières au moyen des technologies et sites de l'Internet. Les huit principes fondamentaux énoncés par l'OCDE dans ses Lignes directrices de 1980 sont les suivants :

1. **Limitation en matière de collecte** : Il conviendrait d'assigner des limites à la collecte des données à 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 à 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 à 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 à caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe (…) [3], 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 à caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.
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 maître du fichier et le siège habituel de ses activités.
7. **Participation individuelle :** Toute personne physique devrait avoir le droit : a) d'obtenir du maître du fichier, ou par d'autres voies, confirmation du fait que le maître 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 maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Malgré la diversité des approches nationales, des préférences des consommateurs et des cadres d'autorégulation élaborés par les entreprises, les Lignes directrices de l'OCDE demeurent l'expression d'un consensus sur la protection des données. Lors de la Conférence ministérielle sur le commerce électronique *Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial*, qui s'est tenue à Ottawa en 1998, l'OCDE a réaffirmé que ces lignes directrices constituaient un fondement international pour la protection de la vie privée.

Il y a longtemps que l'OCDE a reconnu le rôle que la technologie pouvait être appelée à jouer dans le renforcement de la protection de la vie privée dans le cyberespace. En 1997, elle a publié 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*, dans lequel elle encourageait l'élaboration de politiques et de technologies propres à garantir la protection de la vie privée des individus sur les réseaux mondiaux. Les Ministres des pays membres de l'OCDE ont reconnu, dans la déclaration ministérielle d'Ottawa (1998), l'importante contribution que la technologie pouvait apporter à la protection de la vie privée, notant qu'ils prendraient les mesures nécessaires pour « encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée ». La tâche des entreprises, des consommateurs et des pouvoirs publics consiste à mettre effectivement en application les principes énoncés dans les Lignes directrices de 1980 de l'OCDE dans un contexte caractérisé par un changement technologique rapide.

La demande de technologies protectrices de la vie privée

L'utilisation de l'Internet est montée en flèche depuis 1993 avec l'introduction de l'interface utilisateur graphique et la décentralisation de l'administration de l'Internet vers le secteur privé en 1995. L'Internet, qui était auparavant un phénomène essentiellement nord-américain, a alors pris la dimension internationale que l'on connaît aujourd'hui. Favorisée par la déréglementation des télécommunications, la baisse des prix des matériels, des logiciels et de l'accès à Internet, ainsi que par la mise à disposition en ligne de services et produits de plus en plus fiables, la croissance de l'utilisation de l'Internet devrait demeurer vigoureuse dans un avenir prévisible.

L'utilisation de l'Internet varie considérablement, depuis la simple information présentée en ligne jusqu'aux systèmes complexes qui peuvent héberger des milliers de sites Web simultanément. L'internaute peut accéder au cyberespace à partir de son lieu de travail, d'un compte scolaire ou d'un compte personnel par l'entremise d'un fournisseur de services Internet (FSI)[1].

L'utilisation augmentant la viabilité commerciale de l'Internet s'améliore. Depuis plusieurs année, les entreprises de tous les secteurs d'activité, petites sociétés et multinationales, de toutes les régions du monde, se ruent en masse sur l'Internet. De par sa dimension internationale, le « réseau des réseaux » offre aux entreprises un nouvel instrument, attrayant et souvent très rentable, pour renforcer leur présence sur le marché. Internet se prête en effet à la mise en œuvre de modèles commerciaux de plus en plus variés qui éclipsent les solutions catégorielles ou uniformes, dorénavant jugées inapplicables ou, au pire, contre-productives.

Dans le même temps, la collecte de données à caractère personnel a commencé à susciter de plus en plus de préoccupations pour un certain nombre de raisons.

Premièrement, les technologies de pointe permettent de collecter de l'information sur les internautes qui visitent des sites Web, participent à des groupes ou des forums de discussion, expédient un courriel ou utilisent les services Internet d'autres façons, et cela à leur insu ou sans leur consentement. Le plus souvent, les données recueillies ne sont pas à proprement parler des *informations nominatives* au sens où on l'entend généralement, mais plutôt des données essentielles au maintien du système et à la viabilité du réseau. Néanmoins, les consommateurs sont souvent étonnés d'apprendre que ce type d'information peut être collectée à leur sujet.

Le débat sur le respect et la protection de la vie privée se poursuivant dans les médias, au sein des associations de consommateurs et dans les instances les plus diverses, les citoyens sont souvent étonnés d'apprendre combien de renseignements sont recueillis à leur sujet, dans le cyberespace comme dans le monde matériel. Ils ne savent souvent pas à quelle fréquence ils sont filmés par des caméras de surveillance sur des lieux publics, par exemple, ni que des portes automatiques peuvent déclencher le fonctionnement d'un « œil magique », ou encore que les tourniquets des services de transports publics savent compter et surtout, pour les usagers qui utilisent une carte d'abonnement de longue durée, qu'ils enregistrent le nombre de leurs déplacements.

Deuxièmement, il reste beaucoup à faire pour que les citoyens préoccupés par la protection de la vie privée dans le cyberespace aient à leur disposition les instruments nécessaires pour se protéger contre la divulgation d'informations nominatives sans leur consentement. La majorité des sites Web les plus fréquentés affichent des politiques de protection de la vie privée, des secteurs d'activité ont élaboré et mis en œuvre des initiatives d'autorégulation, et certains gouvernements nationaux ont adopté des lois relatives à la collecte des données, mais les enquêtes révèlent que l'inquiétude est encore largement répandue. Ainsi, une étude de la *National Consumers League* réalisée par Harris International en octobre 2000 a révélé que 56 pour cent des personnes interrogées étaient préoccupées par le risque d'atteinte à leur vie privée (*National Consumers League*, 2000). En outre, bien que l'Internet soit devenu de plus en plus convivial ces dernières années, son caractère technique est souvent intimidant pour de nombreux usagers qui s'estiment pratiquement dans l'impossibilité de faire quoi que ce soit pour éviter que des données soient collectées, utilisées ou diffusées sans leur consentement[2].

Troisièmement, s'il est normal que les approches en matière de protection de la vie privée varient selon les pays, cette diversité complique la question pour les autorités, les entreprises et les citoyens. Ainsi, l'Europe et les États-Unis, par exemple, abordent la question de la vie privée selon des optiques très différentes (comme en témoigne le récent accord Europe-USA relatif aux *safe harbours,* ou « sphères de sécurité »), ce qui pose un problème de taille pour les entreprises desservant à la fois des clients européens et américains.

Pour les internautes/consommateurs, la diversité des approches en matière de protection de la vie privée selon les juridictions pose un problème particulier. En effet, le consommateur qui utilise l'Internet ne saura peut-être pas que les sites qu'il visite peuvent être situés dans un autre pays que le sien, et il ne comprendra donc peut-être pas que le dispositif de protection des données auquel il est habitué puisse ne pas être appliqué au site auquel il communique de l'information. Cette situation peut devenir particulièrement préoccupante lorsque le consommateur communique des données sensibles.

Certes, en raison de la diversité des approches et des limites des technologies, aucune de celles-ci ne permet de prendre en compte la multitude de lois sur la protection de la vie privée en vigueur dans tous les pays, régions ou juridictions. Ainsi, il est souvent difficile de déterminer l'origine d'un visiteur qui arrive sur un site Web, le pays d'origine d'un cyberconsommateur, ou encore, du point de vue du site Web, de

s'adapter à un cadre réglementaire et à des préférences de consommateurs qui changent rapidement dans tous les pays du monde. Par conséquent, l'installation de moyens protecteurs de la vie privée sur l'ordinateur personnel du consommateur, configurés en fonction peut-être des préférences personnelles de ce dernier et de la législation nationale applicable, pourrait être une réponse efficace aux préoccupations relatives à la protection de la vie privée, en particulier si cette mesure s'accompagne d'une application et d'une reconnaissance plus larges des principes de protection de la vie privée qui sont acceptés internationalement.

I. Méthodes de collecte des données

La collecte des données peut se faire de diverses façons et nul doute qu'elle sera encore facilitée par les progrès constants de la technologie. A cet égard, la présente liste ne retient que certaines des techniques les plus largement utilisées et ne saurait être considérée comme exhaustive.

En outre, il importe de reconnaître que d'importants progrès ont été réalisés du point de vue de la transparence. En effet, devant les inquiétudes croissantes des citoyens, de nombreux sites Web – et certainement la plupart des plus populaires – affichent maintenant bien en évidence des liens vers leur politique de protection de la vie privée, font ouvertement état de leurs pratiques en matière de collecte de données et fournissent des renseignements sur l'utilisation des données collectées. Ces dernières années, les propriétaires et/ou administrateurs de sites Web ont été de plus en plus nombreux à comprendre que les particuliers non seulement veulent savoir si les sites qu'ils visitent adhèrent à une politique de protection de la vie privée et, dans l'affirmative, quelle en est la teneur, mais que cela déterminera en outre certaines de leurs décisions.

Les technologies et les méthodes de collecte et d'analyse des données peuvent se révéler extrêmement utiles pour faciliter la vie du cyberconsommateur, améliorer les services et développer un contenu, des produits et des services plus personnalisés.

Les sites Web commerciaux recueillent de l'information par des moyens actifs et passifs. La première catégorie comprend les pages d'enregistrement, les enquêtes et d'autres formulaires en ligne. Ce sont des moyens qui font appel à une certaine participation de l'internaute, lequel sait qu'il fournit de l'information et/ou qu'elle est collectée. Les moyens passifs regroupent en général la collecte de données globales et le choix des sites. Il se peut que l'utilisateur ne sache pas que cette information, en général non nominative, est collectée. L'utilisation de témoins de connexion (*cookies*) est souvent qualifiée de passive, mais étant donné que tous les navigateurs proposés sur le marché donnent les moyens à l'internaute de tous les rejeter ou de n'en accepter que certains, uniquement après son approbation, on peut aussi parler d'utilisation active.

Collecte passive de données transactionnelles

Les données non nominatives qui sont divulguées au cours de la navigation sur un site constituent une source importante de renseignements sur les activités en ligne. Les serveurs Web peuvent recueillir de l'information sur les pages qui ont été consultées par un internaute, sur la durée d'affichage d'une page donnée à l'écran, sur l'adresse URL du site visité le plus récemment et sur l'URL du site demandé par la suite[3].

Aucune de ces données n'est en soi nominative. En fait, une grande partie de ces renseignements anonymes sont agrégés et utilisés à des fins de marketing et d'analyse du site. Par exemple, il peut être très utile pour l'opérateur d'un site Web de savoir que sa page d'accueil a été visitée 100 000 fois pendant un

mois par 54 000 visiteurs différents, mais qu'une page consacrée aux promotions de dernière minute ou aux nouvelles sur un sujet donné n'a reçu que 2 000 visites.

Une bonne part de cette information est recueillie pour permettre aux administrateurs de site de remplir les fonctions de maintenance et de vérification, d'optimiser la liaison vers l'ordinateur d'un internaute et la vitesse de connexion, et d'exécuter d'autres tâches techniques. Cette information leur est nécessaire pour s'assurer du bon fonctionnement du site et pour offrir un accès adéquat aux visiteurs. Certains renseignements peuvent être obtenus dans le cadre du fonctionnement normal du logiciel du serveur Web lui-même et stockés dans des fichiers maintenance utilisés pour assurer la fiabilité du système.

Collecte passive d'informations à caractère personnel

Certains renseignements nominatifs peuvent être recueillis par des moyens passifs, surtout si l'usager a configuré son navigateur d'une certaine façon. Des sites Web collectent de l'information auprès des internautes qui stockent par exemple leur adresse électronique ou leur nom dans leur navigateur, sans toujours savoir que ces renseignements sont collectés. Il convient toutefois de noter que la plupart des sites adhérant à une politique de protection de la vie privée qui recueillent ce type d'information le font savoir aux internautes. Ceux-ci peuvent alors éviter que l'information en question soit collectée, tout simplement en ne la stockant pas dans leur navigateur, car elle n'est nécessaire au bon fonctionnement d'aucune application de navigation.

Collecte active d'informations transactionnelles ou personnelles

De nombreux sites procèdent à une collecte active d'informations transactionnelles ou personnelles en mettant en œuvre des technologies ou des processus commerciaux spécifiques. Plusieurs méthodes sont très explicites et nécessitent la participation de l'intéressé à la collecte de l'information, par exemple pour les formulaires en ligne ou les comptes utilisateurs. D'autres méthodes en revanche peuvent être moins évidentes pour un visiteur, comme les témoins de connexion, les mouchards (« *web bugs* ») ou les pisteurs (« *clear.gifs* »).

Comptes utilisateurs

Certains sites Web permettent aux utilisateurs de créer un compte en ligne. En général, l'information concernant ce compte est stockée au site Web même, y compris un nom d'utilisateur et un mot de passe. Les comptes utilisateurs s'adressent souvent aux utilisateurs qui auront vraisemblablement besoin d'avoir accès à de l'information antérieure ou à des données recueillies hors ligne, par exemple dans le cadre d'un programme de fidélisation de compagnie aérienne ou sur le site d'un cyberdétaillant. Lorsque l'utilisateur visite un site, il est en général invité à exécuter la procédure d'entrée en communication, d'habitude en indiquant un mot de passe et un nom d'utilisateur, pour avoir accès à l'information stockée dans son compte.

Pour créer un compte, si les services offerts sur le site sont payants, il faut parfois fournir ses coordonnées de base, ses préférences ainsi que des renseignements sur sa solvabilité. De nombreux sites collectent et tiennent à jour un historique des consultations et des commandes de l'internaute, son parcours ainsi que des informations personnelles nécessaire pour effectuer sa transaction ou donner suite à ses demandes. Des informations sur les préférences des internautes aident également le site Web à déterminer l'offre qui intéresse ses visiteurs et celle qui ne les intéresse pas. Le consommateur peut ainsi y gagner beaucoup en commodité. La collecte de ce type de données est légale et souvent souhaitable pour le

consommateur, et les sites où est appliquée une politique de protection de la vie privée font souvent savoir aux visiteurs qu'ils y ont recours. En tout état de cause, un site qui informe les visiteurs de ses procédures de collecte de données, que ce soit volontairement ou parce que la loi l'y oblige, devrait indiquer ses procédures de collecte de données de parcours (« *clickstream* »).

Étant donné l'importance des investissements en infrastructure et de la maintenance que nécessitent des systèmes de grande envergure, et compte tenu des normes de sécurité qu'il faut y appliquer, ce sont en général seulement les entreprises ayant besoin de conserver cette information sur leur propre serveur pour des raisons opérationnelles qui créent des comptes utilisateurs.

Formulaires en ligne

Les formulaires en ligne sont un moyen courant de recueillir de l'information auprès des consommateurs. Ils se prêtent aux utilisations les plus variées, que ce soit pour collecter des données auprès d'un internaute qui a demandé un complément d'information sur les produits ou services d'une entreprise ou pour effectuer une enquête en ligne. L'utilisation des formulaires est très répandue et son utilité n'est limitée que par l'imagination du concepteur du site.

Il arrive qu'un site demande à un visiteur de s'enregistrer, même si le service, le produit ou le contenu offert est gratuit. En général, l'enregistrement comporte des avantages supplémentaires qui échappent aux utilisateurs non enregistrés. Ainsi, un site de cartes de souhaits électroniques, par exemple, peut permettre aux utilisateurs enregistrés de créer leur carnet d'adresses personnel ou un calendrier de dates importantes, ce qui accroît l'utilité du site pour eux et leur donne une raison d'y revenir.

Souvent, l'enregistrement n'est pas nécessaire pour utiliser un site, mais les services supplémentaires ne sont accessibles qu'aux utilisateurs enregistrés. C'est alors au consommateur de choisir. De nombreux sites de commerce électronique, par exemple, permettront à une personne de passer une commande sans créer un compte, mais celle-ci ne sera peut-être pas en mesure de retourner au site et de profiter de services plus évolués qui sont proposés, comme la vérification de l'exécution de la commande, l'utilisation de certificats-cadeaux ou le stockage d'adresses d'expédition en ligne pour usage ultérieur. Il se peut que le visiteur non enregistré doive fournir de nouveau des renseignements essentiels à chaque visite, qu'il n'ait pas accès aux programmes de fidélisation, ou qu'il lui soit impossible de renouveler une transaction, une navigation ou un achat antérieur, ou encore de modifier ses préférences de cyberconsommateur.

Les avantages que comporte la collecte de cette information pour les entreprises sont évidents. En demandant au visiteur de remplir un formulaire d'enregistrement où il indiquera des renseignements personnels (son nom, son adresse, comment il a entendu parler du site Web, ses centres d'intérêt), les entreprises peuvent établir des profils et des analyses de clientèle extrêmement utiles. Ces données peuvent également leur servir à améliorer le contenu de leurs sites et à perfectionner les services ou produits offerts.

Témoins de connexion

De nombreux sites utilisent des témoins de connexion pour obtenir des renseignements côté client et améliorer l' « expérience-utilisateur ». Les témoins permettent à un serveur Web de stocker et d'extraire de l'information du côté client de la liaison serveur-navigateur (client).

La plupart du temps, les données stockées dans les témoins ne portent pas atteinte à la confidentialité des données personnelles. Il s'agit plutôt d'informations qui sont de première importance pour valoriser sensiblement l'expérience-utilisateur. Un témoin peut par exemple déterminer si un internaute donné a déjà visité le site. Selon l'information stockée, le site peut offrir une information qui s'adresse au nouveau

venu ou bien remercier un visiteur de revenir. Cette information n'est pas forcément nominative, surtout si le navigateur a été utilisé par d'autres ou si l'ordinateur est partagé, par exemple en milieu de travail.

Les témoins améliorent aussi considérablement la fonctionnalité en ligne. De nombreuses fonctions courantes du commerce électronique seraient impossibles sans eux. En voici un exemple. Lorsqu'un consommateur fait des achats sur un site de commerce électronique et ajoute des produits à son cyberpanier, l'information concernant les produits qu'il a identifiés est utilisée pour préparer l'information d'expédition pendant qu'il continue ses courses[4]. L'information au sujet des produits qui se trouvent dans le panier est stockée dans le serveur lui-même, et non dans l'ordinateur du consommateur. Le serveur conserve ensuite le contrôle de l'information concernant le consommateur et ses préférences, tandis que l'ordinateur de ce dernier ne contient que l'information qui permettra au serveur de faire le lien entre l'information de session stockée au site et le consommateur. Ces techniques, regroupées sous l'appellation « gestion d'état », sont nécessaires pour répertorier les utilisateurs et les options qu'ils choisissent. Sans la gestion d'état, il serait impossible de faire du commerce électronique ou d'offrir une expérience-utilisateur transparente.

Les témoins peuvent également être utiles pour s'assurer qu'une page Web est correctement livrée à l'internaute. Les pages Web peuvent être complexes, être composées de textes, de graphiques, d'images, de plans ou d'autres éléments. Pour obtenir chaque page, l'ordinateur de l'internaute doit adresser un certain nombre de demandes distinctes, par exemple, pour la livraison initiale de la page, puis pour les graphiques ou les images, ou les fenêtres incorporées. Les témoins, qui sont stockés dans l'ordinateur de l'internaute, aident le serveur Web à reconnaître qu'une page a été correctement livrée au demandeur.

Les témoins utilisés pour contrôler l'environnement de l'internaute sont en général éphémères. Ils ne sont souvent pas stockés de façon permanente dans l'ordinateur de l'internaute et ne servent qu'au contrôle de la session. En général, ils ne contiennent aucune des informations à caractère personnel.

Les témoins persistants sont stockés jusqu'à leur date d'expiration. Ils contiennent en général une information plus complexe, par exemple concernant la connexion, le numéro de compte ou d'autres données à caractère unique. Les données stockées dans un témoin persistant peuvent être nominatives ou non.

Les témoins facilitent l'utilisation du site Web par le consommateur (contrairement aux comptes utilisateurs ou au stockage d'informations temporaires sur le serveur Web proprement dit) car ils permettent au site d'utiliser les ressources de l'ordinateur de ce dernier plutôt que le serveur. Pour un site qui peut accueillir parfois simultanément des milliers d'utilisateurs, la capacité de partager les ressources informatiques avec chacun améliore le service pour tous.

Cependant, les témoins, comme on le sait, suscitent des critiques. L'une de celles que l'on entend souvent est qu'ils peuvent être installés dans l'ordinateur de l'internaute à l'insu de ce dernier si son navigateur est configuré en ce sens. Les témoins ont suscité des réactions négatives de la part des médias et des défenseurs de la vie privée, et une abondante information erronée à leur sujet est largement diffusée sur l'Internet. Certains voient dans les témoins une intrusion dans la vie privée, d'autres craignent qu'un ordinateur distant ne stocke des données sur leur ordinateur, tandis que d'autres encore croient (à tort) que les témoins peuvent transmettre des virus ou endommager d'une façon ou d'une autre leur ordinateur.

En général, un témoin ne peut fournir de l'information qu'au site Web qui l'a installé à l'origine. Autrement dit, un témoin créé par le site A ne peut pas être lu par un site B. Cette pratique, définie dans plusieurs documents RFC[5], élimine pratiquement le risque qu'un site Web lise de l'information stockée par un autre[6].

Comme beaucoup de moyens technologiques, les témoins peuvent être utilisés pour faciliter la vie du cyberconsommateur, mais aussi à des fins plus délicates à évaluer. Le fait qu'un site installe des témoins n'est en soi ni « bon » ni « mauvais », la technologie étant neutre. Cependant, les témoins sont capables de stocker une quantité appréciable d'information sur les habitudes de navigation d'un internaute, et comme il est possible de les déployer de nombreuses façons différentes, ils peuvent être un motif de préoccupation pour les consommateurs.

Les internautes ont à leur disposition de nombreux outils leur permettant d'exercer un contrôle sur les témoins ainsi que sur l'information collectée par d'autres moyens technologiques. Ceux qui ne s'occupent pas de leurs témoins, ne serait-ce que pour vérifier de temps à autre lesquels sont installés sur leur système, ou qui n'utilisent pas les outils de gestion de témoins trouveront peut-être que certains sites recueillent davantage de renseignements qu'ils ne le souhaiteraient.

Tous les navigateurs courants comportent un outil de gestion de témoins intégré d'un type ou d'un autre qui permet à l'internaute de rejeter tous les témoins, de les accepter tous ou de faire un choix pour chacun d'eux. Les internautes chez qui les témoins suscitent des inquiétudes devraient être encouragés à utiliser ces moyens qui sont accessibles à tous. En outre, tous les navigateurs permettent aux internautes de prendre connaissance des témoins installés sur leur ordinateur et de supprimer ceux qu'ils ne souhaitent plus conserver ou qu'ils jugent choquants. Des sites comme celui du Générateur de déclaration de politique de protection de la vie privée, de l'OCDE, qui pose des questions précises et détaillées sur l'utilisation des témoins, contribuent également à améliorer la transparence de l'utilisation de cette technologie. Pour ceux qui recherchent des moyens technologiques plus robustes, les outils de gestion de témoins sont examinés de façon plus approfondie dans la section ci-après consacrée aux différentes technologies protectrices de la vie privée.

Mouchards et pisteurs (Clear.gifs, 1x1.gifs, Invisible.gifs ou Beacon.gifs)

Les mouchards Web sont de petites images, en général d'un pixel, qui sont souvent placées sur les pages HTML[7] pour tracer la consultation de la page et renseigner à ce sujet la partie qui place l'image dans ces pages.

En général, ces images servent à déterminer combien de visites reçoit une page Web. Les mouchards sont surtout utilisés pour évaluer le trafic sur le Web, déterminer le nombre de fois qu'une page a été consultée, ou pour répondre à d'autres besoins d'ordre administratif ou de surveillance de site. Un système de surveillance d'utilisation révélera combien de fois des internautes ont eu accès à l'image – renseignement standard non nominatif utilisé en maintenance des systèmes. Par ailleurs, ce système peut également servir à demander des renseignements complémentaires, notamment l'URL de la page sur laquelle l'image est installée, le type de navigateur utilisé, la durée de consultation, l'adresse IP de l'internaute, ou pour extraire de l'information stockée dans les témoins. Ces images peuvent être utilisées dans tout code HTML, que ce soit sur une page Web ou sur un courriel HTML.

Étant donné que ces images ne peuvent en général pas être vues ni neutralisées par les bloqueurs de témoins courants[8] ou d'autres techniques analogues, elles ont suscité chez les défenseurs de la vie privée des inquiétudes que l'utilisation accrue de la messagerie HTML n'a fait qu'accentuer.

Navigateurs Web

L'apparition des navigateurs Web a été déterminante pour rendre l'Internet et les réseaux mondiaux accessibles au grand public. Avant l'élaboration de ces navigateurs et du HTML, l'Internet était dans une large mesure limité aux milieux universitaires, aux ingénieurs et aux mordus de l'informatique. Sans les

navigateurs, l'Internet ne se serait jamais développé pour devenir le précieux support d'information que nous connaissons aujourd'hui.

Depuis leur apparition au début des années 90, les navigateurs Web sont devenus de plus en plus complexes et puissants. Ils intègrent maintenant les logiciels clients messagerie et des capacités FTP, et sont compatibles avec des modules d'extension (« *plug-in* »)[9] très divers. En utilisant les caractéristiques des navigateurs Web, certains usagers choisissent de stocker des informations personnelles, par exemple des adresses électroniques ou des noms, dans les préférences qu'ils sont invités à indiquer. Cette information peut être accessible à partir d'un serveur Web ; le navigateur la fournira au serveur qui en fera la demande.

Les utilisateurs de logiciels clients messagerie plus évolués, comme Microsoft Outlook, la messagerie Web, AOL ou d'autres services en ligne propriétaires, n'ont pas à indiquer cette information dans les caractéristiques de personnalisation de leur navigateur. Certains internautes qui font confiance aux logiciels clients messagerie jumelés à des navigateurs doivent indiquer au moins leur adresse électronique pour que l'adresse retour apparaisse ou que l'identité de l'expéditeur soit correctement communiquée aux destinataires de leurs courriels. La possibilité de demander et de recevoir de l'information stockée dans le fichier préférences, si elle a été au départ conçue par souci de commodité, peut néanmoins être à l'origine de la divulgation d'une adresse électronique ou d'autres renseignements que l'internaute aura décidé de fournir.

Les avantages de la collecte de données

Réunis à Ottawa en 1998, les Ministres ont constaté les avantages que comporte le commerce électronique pour toutes les parties prenantes, reconnaissant que pour que ce nouvel espace marchand se développe dans le monde entier, ses utilisateurs devaient unir leurs efforts pour trouver des solutions applicables au nouveau défi que pose un monde sans frontières.

S'agissant de la question de la protection de la vie privée, les responsables de l'action gouvernementale, les défenseurs de la vie privée et l'industrie évoquent souvent l'idée d'un conflit entre les besoins des entreprises en matière d'information sur leurs clients et la volonté des citoyens de contrôler l'information qui les concerne. Cette distinction est quelque peu réductrice et décrit abusivement les entreprises et les consommateurs comme étant en opposition sur la question de la vie privée. En fait, le secteur privé, en même temps que se développaient les technologies de renforcement de protection de la vie privée, militait en faveur de la généralisation des politiques de protection de la vie privée et il a contribué à des initiatives d'autorégulation efficaces.

La section ci-après met en évidence quelques-uns des principaux avantages de la collecte de données.

Commodité pour l'internaute

La collecte d'information au sujet des internautes permet de fournir un service personnalisé à chaque visiteur de site Web. L'Internet répond aux exigences des consommateurs par divers moyens, comme en témoignent les nombreux portails, sites de commerce électronique ou sites d'actualité qui offrent aux visiteurs la possibilité de créer un compte ou d'utiliser d'autres technologies pour individualiser leurs déplacements dans le cyberespace.

Amazon.com, par exemple, peut être programmé pour rappeler le nom d'un client et son historique d'achats. Cette capacité d'accueillir les clients qui reviennent et de créer une page d'accueil individualisée suggérant des produits permet à Amazon.com de fidéliser sa clientèle et de gérer au mieux ses stocks en

envoyant des messages personnalisés qui proposent des produits ciblés ou des offres spéciales fondées sur les préférences des clients. De son côté, CNN.com permet aux internautes de classer par ordre de priorité les sujets d'actualité qu'ils privilégient. De nombreux sites de commerce électronique offrent aux clients de créer des comptes et peuvent y stocker leur numéro de carte de crédit, leur adresse d'expédition et leurs préférences en matière de facturation, ce qui simplifie l'utilisation des fonctions du site ultérieurement. Bon nombre de ces caractéristiques ont leur équivalent dans le monde matériel. Un consommateur aura par exemple beaucoup plus tendance à fréquenter une librairie de son quartier, où l'on connaît ses goûts littéraires, ou le café du coin de la rue, où le garçon le reconnaît et sait comment il aime son café. A bien des égards, la capacité de personnaliser ou d'individualiser les cyberactivités permet de créer pour le consommateur une sorte d'« ambiance de quartier » qui confère une certaine convivialité à ce qui serait autrement une froide transaction commerciale. Mais bien sûr, les consommateurs qui privilégient l'anonymat ou ne souhaitent pas autant de « familiarité » dans leurs déplacements sur la Toile ont aussi le choix.

Toutes ces caractéristiques facilitent les activités de chaque internaute dans le cyberespace en lui rendant l'accès aux sites plus commode et plus rapide.

Un précieux outil de marketing et de développement des entreprises

L'environnement électronique se caractérise par une très vive concurrence, comme de nombreux cyberdétaillants l'ont appris ces derniers mois. L'entreprise doit tout faire pour conquérir une part de marché en fidélisant une clientèle, élargir ensuite cette clientèle et accroître le nombre de transactions par client (autrement dit, engendrer des ventes qui se répètent). Et comme il est beaucoup moins coûteux de conserver un client que d'en trouver un nouveau, l'établissement d'une relation durable avec un client est souvent un facteur déterminant du succès d'une entreprise dans le cyberespace.

Pour développer cette relation, l'entreprise doit impérativement être capable de leur fournir des services personnalisés, de répondre rapidement à leurs préoccupations et de respecter leurs préférences. Pour ce faire, elle doit parfaitement comprendre le marché et les consommateurs, et pour cela il lui est indispensable de recueillir des données sur les clients qu'elle a déjà.

Ces techniques de marketing profitent aux clients. Les grands voyageurs, par exemple, bénéficient de réductions de tarifs ou d'autres avantages lorsqu'ils sont fidèles à une compagnie aérienne. Un site peut offrir un service personnalisé ou stocker les préférences de l'utilisateur. Ces instruments encouragent la fidélité de la clientèle et augmentent les chances de succès du commerce électronique.

Amélioration de l'expérience-utilisateur/protection du consommateur

La collecte de données non seulement facilite la vie de l'internaute par la personnalisation et la prestation de services améliorés à partir d'un site Web donné, mais elle peut également jouer un rôle de premier plan dans la protection des consommateurs et dans l'amélioration de leurs cyberactivités.

Il est utile ici de donner un exemple.

Prenons le cas d'une agence de voyage en ligne auprès de laquelle un client vient d'acheter un billet d'avion pour Paris. Si ce client réserve ensuite une chambre d'hôtel à Rome pour les mêmes dates alors qu'elle est en principe en train de voler vers Paris, le système pourrait lui demander de confirmer l'exactitude des dates de sa réservation d'hôtel à Rome. En allant ainsi au devant des besoins du client, le système peut lui éviter de se voir facturer sans s'y attendre des réservations d'hôtel dont il n'avait pas besoin, ou d'arriver à Paris avec des réservations incorrectes.

II. Technologies protectrices de la vie privée

Bien que l'on reconnaisse l'importance des données à caractère personnel pour faciliter des opérations techniques et commerciales essentielles, l'internaute s'inquiète encore des risques associés à la communication de données le concernant. Ainsi que cela a été noté dans la déclaration ministérielle de 1998 relative à la protection de vie privée sur les réseaux mondiaux, les technologies protectrices de la vie privée peuvent contribuer grandement à la protection de l'information nominative ; en outre, ces technologies dotent l'internaute des moyens nécessaires pour faire des choix éclairés en ce qui concerne la protection de sa vie privée. En lui permettant d'exercer davantage de contrôle sur des informations personnelles qui le concerne, elles contribuent à apaiser bon nombre des inquiétudes que les consommateurs considèrent comme des obstacles à la croissance du commerce électronique.

Les technologies de protection de la vie privée peuvent être très différentes du point de vue de leur fonctionnalité, de leur capacité, de leur structure technique et de leur facilité d'emploi, mais elles ont toutes pour but de permettre à l'utilisateur ou au responsable du service technologie de contrôler la divulgation d'information, la quantité d'information divulguée et les conditions dans lesquelles elle est divulguée.

Cela dit, il importe de savoir que ces technologies ne permettent pas, ni n'ont pour but, de répondre à toutes les préoccupations des consommateurs et des autorités en ce qui concerne la collecte de données. Les technologies protectrices de la vie privée constituent seulement l'un des nombreux moyens à la disposition des consommateurs dans le cyberespace et, comme nous l'avons vu, que ces derniers devraient être encouragés à utiliser si la collecte de données suscite chez eux quelque appréhension.

La principale limite de ces technologies de la confidentialité réside dans le fait que les consommateurs n'y sont pas suffisamment sensibilisés. Une profonde réorganisation s'est récemment opérée dans ce domaine. La détérioration des conditions du marché pour toutes les jeunes pousses, la méconnaissance des technologies protectrices de la vie privée et le peu d'intérêt qu'elles suscitent chez les consommateurs ont entraîné la disparition pure et simple de certaines d'entre elles ou d'importantes modifications. Autrement dit, les consommateurs doivent être au fait de l'existence de ces technologies et de leurs capacités afin de pouvoir en bénéficier, tout comme l'automobiliste qui doit attacher sa ceinture de sécurité pour mieux se protéger en cas d'accident.

Par ailleurs, les consommateurs qui utilisent déjà des technologies protectrices de la vie privée doivent être incités à le faire systématiquement. En effet, de nombreux internautes qui recherchent la facilité et l'efficacité dans leurs cyberactivités cessent rapidement d'y avoir recours, se privant ainsi des avantages qu'ils pourraient en tirer.

Enfin, le consommateur doit choisir la technologie adaptée à ses préoccupations propres, qu'il s'agisse avant tout de conserver l'anonymat, de garantir l'exactitude ou la sécurité des transactions, ou encore d'exercer un contrôle sur ses données personnelles. Comme l'illustre le présent inventaire, le choix de technologies protectrices de la vie privée et d'outils de renforcement de la sécurité est très vaste et le consommateur doit comprendre que tous ne répondront pas à l'ensemble de ses préoccupations. Ainsi, un programme de cryptage de messages électroniques peut être efficace pour préserver la confidentialité de la correspondance électronique, mais ne pourra guère servir à gérer les témoins ou empêcher l'installation d'un mouchard sur une page Web. Pouvoirs publics, associations professionnelles, groupes de défense des consommateurs, autorités chargées de la protection de la vie privée et experts ont tous un rôle à jouer pour faire en sorte que les consommateurs puissent choisir judicieusement les technologies adaptées à leurs besoins.

Inquiétude des consommateurs à l'égard de la collecte de données

La collecte de données inspire aux consommateurs plusieurs inquiétudes.

Partage des données avec des tiers

Les consommateurs qui ont fourni des informations personnelles à un site, une organisation ou une entreprise donné ne veulent pas que cette information soit communiquée à un tiers (c'est-à-dire à quelqu'un avec qui ils ne sont pas en contact ou en relation avec le site, l'organisation ou l'entreprise en question) sans leur consentement ou à leur insu.

Inquiétude au plan de la sécurité

Les internautes craignent souvent que les parties qui collectent les données ne protègent pas suffisamment des informations personnelles contre la divulgation accidentelle ou malveillante. Une sécurité insuffisante ou une information erronée sur le degré de sécurité assuré sont de nature à dissuader les consommateurs de fournir des informations sur Internet. La divulgation, par quelques sites Web populaires, d'informations concernant des consommateurs, notamment leurs numéros de carte de crédit, a fait grand bruit et avivé les craintes du public, sans provoquer pour autant une prise de conscience plus aiguë de la nécessité de la sécurité ou des moyens de l'évaluer.

Connaissance insuffisante de l'utilisation des données

La croissance rapide du commerce électronique démontre que les consommateurs sont disposés à fournir de l'information, même nominative, pour obtenir des services, des caractéristiques de personnalisation ou un contenu individualisé. Cependant, nombreux sont ceux qui s'inquiètent de la façon dont l'information qu'ils fournissent sera utilisée par l'organisation réceptrice. Un consommateur, par exemple, ne s'inquiétera pas de savoir que des informations personnelles qu'il fournit sont utilisées pour créer des pages d'actualité individualisées, mais il sera plus réticent à fournir les mêmes données si elles servent à des fins commerciales tout autres.

Établissement de « profils clients »

Les entreprises utilisent souvent l'information fournie par les cyberconsommateurs pour établir des profils clients. Ces profils peuvent être personnels (c'est-à-dire se rapporter à un consommateur précis) ou globaux (caractéristiques communes à une population donnée). Ils peuvent avoir une utilité pour les consommateurs et simplifier beaucoup leurs activités dans le cyberespace, mais l'idée d'établir un « profil » a eu très mauvaise presse. Certains consommateurs manifestent des réticences à l'idée qu'ils peuvent être catégorisés, et qu'un site Web stocke leur historique d'achats et conserve à leur sujet des renseignements personnels. Ce qui inquiète aussi surtout une partie d'entre eux, c'est le fait que des données collectées sur un site puissent être combinées avec de l'information hors ligne ou des données obtenues d'autres sites ou magasins électroniques.

Usurpation d'identité

La communication d'informations particulièrement sensibles, à caractère financier par exemple, est un motif de grande préoccupation pour de nombreux consommateurs et décideurs. L'utilisation abusive des informations personnelles peuvent dans certains cas relever de l'usurpation d'identité. L'usurpation est un délit qui peut certes être commis autant dans le monde hors ligne que dans le cyberespace, mais on constate que le phénomène a pris de l'ampleur ces dernières années. On ignore dans quelle mesure cette progression est due à une sécurité défaillante des données, à une augmentation du vol ou de l'utilisation abusive d'information, ou simplement au fait qu'il est plus facile d'avoir accès à l'information nécessaire pour s'approprier l'identité d'un individu sur les réseaux mondiaux. Quoi qu'il en soit, la prise de conscience de ce délit que constitue l'usurpation d'identité n'aura pas manqué de renforcer les réticences de certains consommateurs à communiquer des informations personnelles.

Sécurité et vie privée

Il existe bien sûr une étroite relation entre les technologies de la sécurité et les technologies de la protection de la vie privée. Cette relation étroite est à l'origine d'une confusion assez largement répandue. Les deux concepts ne sont pas vraiment séparés et, s'agissant de la protection des informations personnelles, ils ne sauraient l'être, mais ce ne sont pas pour autant des concepts technologiques interchangeables.

Dans ses Lignes directrices de 1980, l'OCDE a reconnu que la sécurité constituait un élément fondamental de la protection de la vie privée. Sans une sécurité stricte, des informations à caractère personnel ne peuvent pas être convenablement protégées contre l'utilisation malveillante ou abusive.

Il importe de noter que lorsqu'on parle de sécurité dans les milieux technologiques[10], on entend en général la protection des données contre la divulgation accidentelle, l'utilisation abusive et la destruction ou l'altération des données, nominatives ou non. La sécurité peut s'appliquer au stockage, à la transmission, à la sauvegarde ou à d'autres opérations effectuées sur des données. Les solutions, produits et services utilisés pour assurer la sécurité nécessaire visent en général à prévenir l'inoculation de virus, à supprimer les points vulnérables du réseau, à limiter l'accès à des usagers autorisés ainsi qu'à authentifier les données, les messages ou les usagers.

Ces instruments revêtent une importance primordiale pour la protection des informations personnelles stockées ou transmises. Si l'on est dans l'impossibilité de sécuriser les données personnelles, un individu ne peut avoir la garantie que les données qui le concernent seront correctement protégées une fois qu'elles seront communiquées à un site, une entreprise ou une organisation dans le cyberespace. Sans les technologies de la sécurité, il serait difficile – voire impossible – de protéger les données et de mettre des outils de protection de la vie privée à la disposition des citoyens, des sociétés et des organisations. La capacité d'offrir au consommateur des choix en ce qui concerne la collecte des données et de sécuriser les données recueillies ou stockées repose sur la disponibilité généralisée de technologies de sécurité fortes.

Au-delà de la nécessité de protéger les données à caractère personnel par des sauvegardes raisonnables ou adéquates, la protection de la vie privée comprend des limites de nature « légale » à la collecte, au traitement, au stockage ou à la transmission de données nominatives ou globales recueillies auprès des utilisateurs. Y a-t-il collecte d'information ? Comment l'information collectée est-elle utilisée ou partagée ? De quelles options dispose l'intéressé ? A-t-il ou non accès à l'information stockée ? Et qui a accès à cette information ? Voilà autant de questions qui alimentent le débat sur la protection de la vie privée.

Technologies protectrices de la vie privée

Il importe de ne pas perdre de vue que les préférences en matière de protection de la vie privée peuvent être aussi différentes que les préoccupations et prérogatives des citoyens à l'égard du traitement des informations personnelles. A noter également que dans l'inventaire ci-après des technologies et des choix qui s'offrent au consommateur, on trouvera des outils logiciels qui s'installent sur le disque dur de l'internaute, d'autres qui sont déployés à l'échelle du réseau fréquenté par l'internaute ou d'autres encore qui sont des services en ligne. Par conséquent, même lorsqu'il a recours à des services en ligne protecteurs de la vie privée ou télécharge un logiciel ayant la même fonction, l'internaute doit veiller à examiner attentivement la politique de protection de la vie privée du site hébergeur ou fournisseur.

Gestionnaires ou bloqueurs de témoins

Les gestionnaires ou les bloqueurs de témoins sont des applications qui permettent à l'internaute de savoir quand des témoins sont installés dans son disque dur, de gérer l'acceptation des témoins et de savoir quelle information est stockée dans chaque témoin. Leur facilité d'emploi et leurs caractéristiques varient beaucoup, mais ils permettent tous à l'utilisateur d'exercer davantage de contrôle sur les témoins stockés sur son ordinateur personnel.

Les gestionnaires ou bloqueurs de témoins peuvent aider l'internaute à déterminer les sites qui ont installé des témoins sur son ordinateur, le moment où les témoins ont été installés et la date d'expiration de ces témoins. Ils permettent également de supprimer ou de conserver un témoin précis. Cependant, étant donné que les données stockées dans de nombreux témoins sont indéchiffrables pour l'utilisateur moyen, les gestionnaires de témoins peuvent être d'une efficacité ou d'une facilité d'emploi limitée pour l'utilisateur qui souhaite connaître exactement l'information stockée dans les fichiers de témoins de son ordinateur.

Il importe de noter que tous les navigateurs commerciaux permettent à l'internaute de déterminer s'il souhaite ou non recevoir des témoins. Il n'a pas à en faire la demande expresse car cette fonctionnalité est inhérente au navigateur. En outre, étant donné que les témoins sont simplement des fichiers texte, tout utilisateur peut lire un témoin stocké sur son disque dur. Cependant, les données stockées dans les témoins sont en général difficiles, voire impossible à comprendre pour l'utilisateur moyen car elles sont parfois codées pour simplifier les communications avec le site Web qui est à l'origine de l'installation du témoin[11].

On trouve sur le marché un vaste choix de gestionnaires de témoins, dont plusieurs en logiciels gratuits ou logiciels partagés.

Bloqueurs de publicité

Pour les internautes qui n'apprécient pas et ne veulent pas recevoir la publicité ciblée qui émane de nombreux sites, il existe également des logiciels qui bloquent la livraison de cyberpublicité. Ils empêchent la publicité d'atteindre l'utilisateur final et, par conséquent, de pister un client. Cependant, étant donné que la publicité peut se présenter sous des formes très diverses, ces applications ne sont pas d'une totale efficacité.

Ce genre de logiciel est indiqué pour les internautes qui utilisent des connexions lentes et ne veulent pas faire mauvais usage d'une largeur de bande précieuse en téléchargeant de la publicité. Le logiciel de blocage présente également un avantage pour ceux qui sont fondamentalement opposés à la cyberpublicité ou qui veulent éviter que leurs enfants ou d'autres utilisateurs y aient accès. Bien qu'il existe plusieurs produits sur le marché, l'utilisation des logiciels de blocage de publicité est relativement limitée. Ce qu'il

importe de savoir, c'est que la publicité ne permet pas en soi de collecter beaucoup des informations personnelles au sujet de la personne qui la consulte.

Logiciels de cryptage

Les logiciels de cryptage permettent à l'internaute de crypter – ou de brouiller – des données numériques. L'internaute peut utiliser le cryptage pour protéger le contenu de ses courriels, des fichiers qu'il a stockés et de ses communications dans le cyberespace. Une fois l'information cryptée, elle ne peut être décryptée qu'à l'aide de la clé numérique appropriée. Cette clé numérique se présente le plus souvent sous la forme d'une marque qui peut être incorporée aux navigateurs, aux identificateurs biométriques, aux cartes à puce et à d'autres dispositifs de stockage, selon la complexité de l'application en cause. Les logiciels de cryptage varient beaucoup du point de vue de leur « force »[12] et de leur fonctionnalité.

Les produits de cryptage qui associent matériel et logiciel sont également populaires, surtout pour les communications complexes ou évolués, les équipements de télécommunications, les systèmes de protection de droits d'auteur, l'identification biométrique, les cartes à puce ou certains produits pare-feu. S'agissant de protection individuelle, les solutions mixtes matérielles-logicielles sont toutefois encore rares.

Les logiciels de cryptage peuvent être très utiles pour l'utilisateur privé. Non seulement le cryptage protège les fichiers stockés, mais il peut également être utilisé aux fins d'authentification et pour assurer la confidentialité des communications. C'est un instrument puissant auquel on peut faire appel dans diverses circonstances pour assurer la protection de la vie privée et la sécurité de l'utilisateur privé.

Dans le même temps, les utilisateurs qui ne connaissent pas bien les technologies de pointe trouveront les produits cryptographiques difficiles d'emploi. Même les produits relativement perfectionnés et conviviaux conçus pour le marché de détail peuvent être déroutants pour l'utilisateur qui n'est pas vraiment au fait des capacités techniques des technologies de la cryptographie. Les éditeurs de logiciels ont mis au point des produits très divers. Une utilisation efficace de la cryptographie exige en général un certain effort de l'internaute.

Ces réserves faites, les produits de cryptage et l'intégration de la cryptographie aux applications standard du consommateur créent un instrument efficace et rationnel qui peut sensiblement améliorer la protection de la vie privée ainsi que la sécurité des données personnelles. L'autonomisation des internautes au moyen de technologies efficaces protectrices de la vie privée passe par la mise à disposition et la facilité d'emploi du cryptage fort.

Les logiciels de cryptage sont largement répandus et existent sous de nombreuses formes : cryptage du disque dur ou cryptage de fichiers, cryptage de messagerie, pare-feu personnel, instruments d'authentification et utilitaires de communications.

Technologies Web

Anonymiseurs

Les anonymiseurs sont des services Web qui agissent comme intermédiaire entre l'internaute client et les sites Web et permettent ainsi de surfer en tout anonymat. En général, un service anonymiseur empêche un site Web d'identifier l'adresse IP du visiteur ou d'implanter des fichiers témoins sur son ordinateur. Cependant, et précisément pour cette raison, les anonymiseurs peuvent également empêcher un internaute d'avoir accès à des services personnalisés ou de tirer parti de certaines fonctionnalités qui nécessitent le

maintien de témoins persistants pour être utilisées correctement, telles que l'accès aux comptes en ligne ou la consultation des historiques d'achats.

Les anonymiseurs peuvent être extrêmement utiles aux consommateurs qui naviguent sur le Web ou qui veulent expédier un courriel anonyme. Simples et faciles d'emploi, ils sont largement répandus sur le Web, et il est souvent possible d'en obtenir une version gratuitement. Pour l'internaute qui tient à conserver l'anonymat sur le Web, les anonymiseurs constituent un excellent choix.

Il y a lieu de noter cependant que les anonymiseurs ne garantissent pas nécessairement que des informations à caractère personnel ne seront pas divulguées. En effet, ce n'est pas parce qu'une transaction est anonyme qu'elle est privée. Du fait que l'anonymiseur agit comme intermédiaire entre l'internaute et les sites Web ou d'autres services Internet qu'il utilise, les données qui figurent dans un fichier journal serveur pourraient être utilisées pour reconstituer ses habitudes de navigation. Les services anonymiseurs appliquent des politiques qui empêchent ces pratiques – par exemple en détruisant régulièrement leurs fichiers journaux Web et en ne conservant pas de copies des fichiers systèmes qui pourraient divulguer des informations personnelles ou servir à identifier quelqu'un – mais ils ne sont pas à toute épreuve.

En outre, les anonymiseurs sont un motif d'inquiétude chez les responsables de l'exécution des lois et dans les autres services chargés de veiller à l'utilisation responsable du cyberespace. En effet, parce que les anonymiseurs peuvent dissimuler l'identité – ou tout au moins la rendre très difficile à établir –, ils suscitent des préoccupations quant à la responsabilité ou à la possibilité de faire respecter les politiques régissant l'utilisation du cyberespace.

Les services de messagerie anonyme sont également couramment utilisés. Ils permettent à l'internaute d'envoyer des courriels sans révéler sa propre adresse électronique ou l'adresse électronique d'origine. On trouvera une page ressource à ce sujet à www.publius.net/rlist.html.

Platform for Privacy Preferences Project (P3P)

La plate-forme d'expression de choix en matière de respect de la vie privée (« *Platform for Privacy Preferences Project* » ou P3P) est une norme élaborée par le *World Wide Web Consortium* (W3C) qui a été proposée pour donner aux internautes les moyens d'exercer davantage de contrôle sur les informations personnelles qui les concernent en permettant aux navigateurs et aux serveurs P3P d'analyser les politiques en matière de respect et de protection de la vie privée. La norme P3P proposée est fondée sur le langage XML[13], qui permet la création d'un vocabulaire commun pour définir les pratiques en matière de vie privée.

Étant fondée sur le langage XML, la norme P3P permet aux navigateurs et aux serveurs de « négocier » avant de donner suite à une demande de livraison de données. Une fois qu'une page Web est demandée par un navigateur donné, par exemple, celui-ci ne livrera la page à l'internaute demandeur que si les choix indiqués dans le navigateur correspondent au site Web. Étant donné que les préférences d'un consommateur sont fixées par l'intéressé et que les politiques du site sont définies par le P3P, le consommateur n'a pas besoin d'analyser les politiques en matière de protection de la vie privée de chaque site qu'il visite.

Une entreprise définit sa politique en matière de protection de la vie privée selon les termes établis par la norme P3P. On y trouve notamment les éléments suivants : POLITIQUE, ENTITÉ, DIVULGATION, RECOURS, DIFFÉRENDS, DÉCLARATION, CONSÉQUENCE, OBJECTIF, DESTINATAIRE, CONSERVATION, GROUPE DE DONNÉES et DONNÉES. Chaque élément est assorti d'attributs indispensables qui définissent plus précisément la politique en matière de protection de la vie privée du site concerné. La combinaison d'éléments de base et de différents attributs confère une grande souplesse au

système, à la fois pour les sites Web et pour les consommateurs. Disposant d'un large éventail de combinaisons possibles d'éléments et d'attributs, les consommateurs peuvent formuler leurs préférences en tenant compte très précisément de leurs choix personnels et les communiquer aux sites Web compatibles avec la norme P3P.

Pour aider les entreprises à mettre au point des produits conformes à la norme P3P, plusieurs sociétés ont créé des éditeurs et des outils d'élaboration de politique P3P qui simplifient grandement la mise au point de produits conformes.

L'internaute, de son côté, doit disposer d'un logiciel qui permet à son navigateur de traduire et de comprendre la spécification P3P. Une fois configurée selon les préférences de l'internaute, l'interaction de P3P entre les serveurs et l'intéressé peut être dans une large mesure transparente, ce qui simplifie l'utilisation. Là encore, de nombreuses entreprises mettent au point des outils P3P côté client qui sont de plus en plus largement répandus.

La norme P3P progresse rapidement et est utilisée dans un nombre croissant d'environnements, et cela pour un certain nombre de raisons.

Premièrement, elle permet à une entreprise de définir sa politique en matière de vie privée en faisant appel à la technologie. Cela permet de répondre à l'une des préoccupations les plus fondamentales de nombreux défenseurs de la vie privée, à savoir que de nombreuses politiques en la matière sont difficiles à comprendre pour les citoyens ou que ces derniers ne mesurent peut-être pas toutes les implications du langage juridique ou spécialisé souvent utilisé dans ces politiques. La norme P3P met un terme à la confusion car elle repose sur l'utilisation de termes fixes.

Elle permet également à l'internaute de définir par des moyens technologiques ses préférences en matière de protection de la vie privée. Celui-ci peut en effet configurer son logiciel en fonction de l'information qu'il souhaite le cas échéant révéler et de l'usage qui pourra en être fait. Cette souplesse permet également à l'internaute de fixer les limites de la collecte de données nominatives selon ses critères. La capacité d'un consommateur utilisant la norme P3P de créer un profil de ces critères en matière de protection de la vie privée qui corresponde à ses préférences personnelles, nationales ou culturelles lui confère une grande autonomie pour ses activités dans le cyberespace.

Deuxièmement, la norme P3P ne nécessite guère d'intervention permanente de la part de l'internaute. En effet, une fois que celui-ci a configuré son ordinateur, l'analyse des politiques en matière de vie privée sur les sites Web compatibles avec la norme est relativement transparente. Selon la fonctionnalité du logiciel client P3P, l'internaute peut occasionnellement déroger à ses préférences afin d'avoir accès à un site qui n'est pas conforme à la norme P3P, mais il peut être assuré que les préférences qui auront été configurées seront respectées en permanence.

Troisièmement, la norme P3P respecte la capacité des entreprises et des citoyens d'élaborer des pratiques différentes en matière de protection de la vie privée. Elle est souple et permet à une entreprise de définir ses pratiques et à l'internaute de définir ses préférences en matière de collecte de données. Elle confère à ce dernier l'autonomie nécessaire pour créer un ensemble unique de préférences et, en même temps, offre les moyens technologiques de veiller au respect de ces préférences.

La norme P3P est encore une technologie émergente dont la viabilité reste à démontrer dans un marché en évolution rapide. De nombreuses entreprises se sont engagées à l'intégrer à leurs lignes de produits, mais la mise en application de la norme demeure relativement limitée.

L'adoption restreinte de la norme P3P par le marché à ce jour tient à ce que le processus de normalisation dans le secteur privé continue d'évoluer, mais elle s'explique également par la nécessité de

respecter le fait qu'une diversité de modèles commerciaux coexistent sur l'Internet, ainsi que le rythme traditionnel des technologies qui sont fortement influencées par les effets de réseau. Les consommateurs qui utilisent des instruments clients P3P vont trouver qu'il n'y a pour le moment que relativement peu de sites qui appliquent les politiques de protection de la vie privée P3P. S'ils limitent leurs préférences exclusivement aux sites conformes à cette norme, ils trouveront peut-être que leurs possibilités de navigation sont limitées. De leur côté, les entreprises qui envisagent d'adopter la norme P3P jugeront peut-être qu'étant donné l'utilisation limitée de l'outil client P3P, l'investissement que nécessiteraient le réaménagement de leur propre site Web et de leurs pratiques en matière de protection de la vie privée ne se justifie pas à ce stade.

Les effets de réseau dans le marché de la technologie sont bien connus. Inévitablement, il faudra un certain temps avant que l'utilisation de la norme P3P se généralise. Cela dit, étant donné l'appui d'un organisme clé de normalisation de l'Internet (W3C) ainsi que la large adhésion que la norme P3P recueille auprès des milieux technologiques, des associations de consommateurs et des défenseurs de la protection de la vie privée, nombreux sont ceux qui estiment qu'elle atteindra sa masse critique sous peu.

On trouvera une liste de sites participants à l'adresse www.w3.org/P3P/compliant_sites.

Réseaux confidentiels

Comme les anonymiseurs et les serveurs mandataires, les réseaux confidentiels (« *privacy networks »)* empêchent les sites Web de voir l'identité de leurs visiteurs. Cependant, ces réseaux comportent souvent d'autres caractéristiques qui les distinguent des anonymiseurs, lesquels sont des dispositifs relativement simples.

Les réseaux confidentiels reposent en général sur l'utilisation de pseudonymes ou de nouvelles identités. L'internaute possède chez un fournisseur de ce type de service un compte qui contient sa véritable identité. Le service lui attribue un pseudonyme, qui peut inclure ou non une information démographique précise. L'internaute utilise alors le réseau d'abonnés pour héberger sa page d'accueil, et comme point de départ pour naviguer sur le Web. Le réseau confidentiel ne révélera que le pseudonyme aux sites Web visités.

En général, les réseaux confidentiels offrent aux internautes un choix relativement vaste quant à l'information qui sera révélée à leur sujet. Certains peuvent décider par exemple d'inclure de l'information démographique de base, permettant ainsi aux sites Web qu'ils visitent de connaître leur âge, leur sexe ou leur lieu de résidence; d'autres, au contraire, décideront de bloquer la diffusion de ces renseignements.

Un réseau confidentiel conservera habituellement les témoins destinés à l'internaute, empêchant ainsi qu'ils soient installés sur l'ordinateur de ce dernier. L'internaute peut par conséquent bénéficier des avantages des services personnalisés et d'autres commodités sans avoir à conserver cette information sur son matériel personnel.

Les réseaux confidentiels peuvent être des services Internet, auxquels l'internaute s'abonne et a accès par l'entremise de son propre fournisseur de services Internet. Il existe également certains réseaux confidentiels qui mettent leurs technologies à la disposition de grands clients professionnels, notamment des sociétés spécialisées dans la protection de la vie privée, qui souhaitent limiter la divulgation d'informations privées concernant leur personnel à des tiers, ou à des fournisseurs de services Internet qui souhaitent incorporer ces services dans leurs propre offre de services.

Pour de nombreux internautes, les réseaux confidentiels laissent entrevoir des perspectives prometteuses car ils leur permettent de tirer avantage des services de personnalisation sans risquer

d'intrusion dans leur vie privée. Les consommateurs comprennent en général que les entreprises ont besoin de données concernant leurs marchés et que ces données leur sont utiles pour améliorer leurs produits et services. La possibilité pour le consommateur de se créer une nouvelle identité correspondant à ses choix et préférences et à l'information démographique nécessaire, sans avoir à divulguer davantage de renseignements personnels à un site en ligne – par exemple l'adresse du domicile ou le numéro de téléphone – est attrayante. Beaucoup voient dans les réseaux confidentiels un instrument efficace pour concilier ces intérêts concurrents.

Dans le marché des entreprises, de nombreux fournisseurs de réseaux et de services Internet considèrent le fait d'utiliser les technologies de réseaux confidentiels comme un avantage qu'ils peuvent répercuter à leur clientèle et qui bonifie leur offre. L'intégration de ces technologies à un réseau d'entreprises ou à un réseau de FSI est techniquement complexe et exige en général un investissement important, mais beaucoup d'entreprises sont d'avis que cet investissement se justifie pour répondre aux préoccupations des consommateurs et les aider à faire des choix éclairés en ce qui concerne la protection de leur vie privée et de leurs données.

Courtiers en information

Les courtiers en information – souvent appelés *« infomédiaires »* – sont des entreprises qui agissent en qualité de courtier pour des informations à caractère personnel. Étant donné que ce segment du marché est en évolution, le concept peut recouvrir plusieurs formules différentes et l'on se bornera ici à en donner un aperçu général.

Le système du courtier en information ou de l'infomédiaire a été à la fois vivement critiqué et largement salué comme une nouvelle possibilité viable pour les personnes soucieuses de protéger leur vie privée. La présente note ne porte pas de jugement sur les modèles commerciaux de ces entreprises. Compte tenu du fait que certains observateurs de l'industrie considèrent cette formule comme un nouvel élément qui améliore le dispositif de protection de l'information nominative, il est noté que ces instruments répondent à la définition de base des technologies protectrices de la vie privée, dans la mesure où ils ont pour but de permettre aux consommateurs d'exercer davantage de contrôle sur la divulgation des informations personnelles qui les concerne.

Les services des courtiers ou infomédiaires sont en général fournis sous forme d'abonnement ou de services payants. L'internaute ouvre un compte auprès d'un courtier, qui suivra par la suite, au moyen de logiciels adaptés, son parcours dans le cyberespace, y compris ses habitudes de navigation, son historique d'achat et d'autres données. C'est le courtier qui constitue la principale source de ce type de renseignements.

En revanche, c'est l'internaute qui conserve le contrôle de l'information et qui peut ordonner au courtier de communiquer de l'information à un site donné et de la refuser à un autre. Le courtier agit au nom de l'internaute, et non du fournisseur, et il peut lui permettre de profiter d'importants avantages et commodités en raison de la richesse de l'information collectée. En outre, les courtiers sont d'importantes sources de données démographiques pour les services de marketing des entreprises, qui peuvent être intéressés à analyser l'information non nominative concernant un segment donné du marché. L'analyse des données permet au courtier de fournir de l'information démographique sans devoir révéler de données nominatives.

Si l'internaute ne souhaite plus utiliser les services du courtier, il peut résilier le service ou l'abonnement, à la suite de quoi l'information concernant l'internaute est en général retirée de la base de données du courtier.

Les agents intelligents ou inforobots *(« bots »)*, qui sont des applications pouvant agir au nom du consommateur en se fondant sur les préférences qu'il a exprimées, sont similaires, mais ils ne seront pas étudiés en détail ici.

Selon certains défenseurs de la protection de la vie privée, s'il est vrai que le système de courtier peut autonomiser les internautes, il subsiste des risques non négligeables car les courtiers ne sont en général pas soumis à réglementation (sauf dans la mesure où ils recueillent des informations sensibles ou réglementées) et le consommateur doit s'en remettre à la politique que déclare suivre une entreprise privée quant à la protection effective dont bénéficieront ses données. Ceux qui sont d'avis que le concept constitue une solution viable pour les consommateurs notent que le modèle commercial d'un courtier dépend entièrement de la relation de confiance qu'il sera capable d'établir avec les consommateurs. Selon eux, c'est le marché qui veillera en définitive à ce que ces entreprises ne portent pas atteinte à la vie privée de leurs clients. Les puissantes forces à l'œuvre dans un marché concurrentiel inciteront fortement ces entreprises à respecter rigoureusement les préférences des citoyens qu'elles représentent.

Le secteur des courtiers en information est encore un marché relativement limité, et l'on ignore si les consommateurs qui ne font pas confiance à une entreprise affichant une politique de protection de la vie privée sur son site Web feront davantage confiance à un courtier pour collecter leurs données personnelles.

Technologies réseau

De nombreuses technologies protectrices de la vie privée peuvent être mises en œuvre sur des réseaux d'entreprise, des LAN ou des WAN privés. Ces technologies permettent aux gestionnaires de ces réseaux de limiter l'information révélée par des individus sur un réseau donné.

Serveurs mandataires et pare-feu

Les serveurs mandataires et les pare-feu sont des technologies qui interviennent en général entre le consommateur et l'Internet. Dans une entreprise, ils peuvent se situer sur le réseau local au point d'interconnexion avec l'Internet, chez le FSI, ou n'importe où entre les deux. Les serveurs mandataires et les pare-feu peuvent également grandement améliorer la sécurité dans un environnement réticulaire.

Les pare-feu et les serveurs mandataires sont assez semblables du point de vue de leur fonctionnalité, bien que les premiers comportent habituellement des caractéristiques de sécurité supplémentaires que l'on ne retrouve pas dans les seconds[14]. En général, les deux technologies permettent cependant d'éviter la divulgation de l'adresse IP d'un individu ou d'autres informations personnelles le concernant en agissant comme intermédiaire entre un site Web et un ordinateur personnel.

Les pare-feu et les serveurs mandataires se distinguent principalement par la façon dont ils livrent l'information à un navigateur. L'information demandée à travers le pare-feu – qu'il s'agisse d'une page Web ou de lecture vidéo en transit – est livrée directement à l'utilisateur. Le pare-feu peut procéder à la détection de virus, appliquer des restrictions à certains types de contenu ou mettre en œuvre des caractéristiques de sécurité complémentaires, mais l'information est renvoyée à l'ordinateur qui a demandé les données à l'origine.

Le serveur mandataire, lui, agit au nom de l'internaute et dissimule l'identité de son ordinateur au site Web. Lorsque l'internaute demande une page Web donnée – www.oecd.org, par exemple –, il transmet en fait la requête au serveur mandataire, lequel à son tour adresse la demande au serveur Web de l'OCDE proprement dit. Ce dernier, dans cet exemple, livrerait la page et l'information demandées au serveur mandataire, lequel ferait suivre à l'internaute demandeur.

Ces technologies sont largement répandues dans les réseaux d'entreprise. Il est facile de se les procurer, souvent jumelées avec le réseau, le site Web et d'autres produits et services Internet. Les pare-feu pour PC sont également très répandus sur le marché de détail des logiciels. Comme ces produits ont été à l'origine mis au point à des fins de sécurité, ils n'offrent souvent pas la même fonctionnalité ou la même souplesse que d'autres produits conçus expressément pour répondre aux préoccupations concernant la protection de la vie privée. Cependant, leur large utilisation continuera d'en faire au moins un élément essentiel de toute solution technologique protectrice de la vie privée.

Les serveurs mandataires et les pare-feu sont faciles à obtenir auprès des entreprises de sécurité informatique et sont souvent jumelés aux logiciels réseau ou Web.

Réseaux confidentiels

Les réseaux confidentiels ont déjà été décrits en détail plus haut. Il convient cependant de noter que de nombreux entreprises qui œuvrent dans ce secteur travaillent avec des fournisseurs de services Internet, des sociétés, ainsi que des sites Web populaires pour incorporer les technologies des réseaux confidentiels et fournir ces types de services à leurs propres personnels, clients ou abonnés. Les réseaux confidentiels ne se limitent donc pas forcément à des services Internet destinés aux consommateurs, mais peuvent être intégrés aux réseaux fermés de diverses organisations ou entreprises.

Par ailleurs, de nombreux prestataires de services en ligne offrent à leurs clients de nouvelles capacités qui leur permettent d'exercer davantage de contrôle sur leurs données personnelles. Les services *Passport* de Microsoft et *Magic Carpet* d'AOL – qui proposent tous deux de nouvelles options au consommateur sur la façon dont chaque service utilisera les données à caractère personnel le concernant – simplifient beaucoup la vie dans le cyberespace en rappelant les préférences des consommateurs, en éliminant la nécessité de fournir de nouveau des renseignements répétitifs et en contribuant à améliorer la convivialité et la transparence des activités en ligne. Si le très vaste déploiement de ces services – *Passport,* par exemple, est mis en œuvre sur les sites Microsoft, mais aussi sur les autres – a suscité certaines préoccupations, la commodité offerte à l'internaute sur tous ses sites préférés se révèle souvent très convaincante. Toutefois, comme avec tout service en ligne, l'utilisateur devrait attentivement vérifier, examiner et évaluer les options qui s'offrent à lui dans la politique de protection de la vie privée du service en question pour s'assurer que les utilisations et les choix proposés ne lui posent pas de problème.

III. Recommandations

La Déclaration ministérielle de 1998 a établi que les technologies protectrices de la vie privée pouvaient jouer un rôle décisif en permettant aux internautes d'exercer un contrôle accru et plus souple sur des informations personnelles les concernant. L'OCDE n'a cessé, depuis, de réitérer l'importance de ces technologies dans de nombreux documents conférences, déclarations et notes, maintes fois évoqués dans le présent document. Les pouvoirs publics et le secteur privé ont un rôle important à jouer en encourageant l'utilisation des technologies protectrices de la vie privée.

L'utilisation des technologies protectrices de la vie privée dans l'application des lois nationales

Les responsables de l'action gouvernementale se demandent depuis longtemps si les technologies protectrices de la vie privée peuvent contribuer à l'application des lois relatives à la protection des données et, dans l'affirmative, dans quelle mesure la technologie peut résoudre les problèmes posés dans ces lois. Jusqu'à un certain point, la réponse à cette importante question est oui, les technologies protectrices de la vie privée peuvent être très utiles à cet égard. Cependant, il importe de bien comprendre que ces

technologies ne sauraient à elles seules satisfaire à tous les critères énoncés dans les textes législatifs sur la protection des données.

Elles peuvent sensiblement autonomiser les consommateurs préoccupés par la collecte de données. La protection de la vie privée est une question qui est par essence personnelle et les consommateurs peuvent avoir chacun des critères très différents en la matière. Les législations nationales peuvent certes fixer des règles de base pour la protection des données, mais les consommateurs auront forcément leurs préférences propres quant aux données qui pourront ou ne pourront pas être collectées à leur sujet. C'est là que peuvent intervenir les technologies protectrices de la vie privée comme important complément des lois nationales de protection des données pour les consommateurs qui éprouvent des inquiétudes particulières ou qui préfèrent une meilleure protection de leur vie privée que ce que prévoit la législation générale.

Dans le même temps toutefois, les technologies ne peuvent être l'instrument d'application de toutes les lois nationales de protection des données ni même des lignes directrices internationales de portée générale. Il existe en effet trop de différences entre les lois nationales, d'exceptions dans certains cas, de nuances ou de traitement différents pour des types de données très divers et pour chaque technologie particulière (ou même combinaison de technologies) pour pouvoir satisfaire à la pléthore de règlements qui accompagnent inévitablement les lois de protection des données. En général, les applications et technologies logicielles répondent à des préoccupations très spécifiques, tandis que les lois de protection des données vise des données à caractère personnel très diverses dans des circonstances très variées. Par conséquent, les technologies protectrices de la vie privée ne sont guère adaptées pour mettre en œuvre des dispositions législatives nationales qui sont de portée souvent très générale et étendue.

Néanmoins, ces technologies peuvent jouer un certain rôle. Le Comité européen de normalisation (CEN) a entrepris une étude approfondie visant à déterminer si des normes technologiques peuvent servir à mettre en œuvre la directive de l'UE relative à la protection des données. Il serait peut-être possible d'utiliser les technologies protectrices de la vie privée pour appuyer la mise en œuvre de cette directive (mais pas forcément de les utiliser dans le cadre législatif américain ou d'autres législations nationales), ce qui pourrait encourager l'élaboration d'autres normes axées sur différentes initiatives réglementaires.

Les technologies protectrices de la vie privée devraient donc être considérées par les pouvoirs publics et les consommateurs comme un outil secondaire de protection. Sans un engagement du consommateur - qui devrait notamment vérifier les politiques de protection de la vie privée et définir ses préférences à cet égard – ces technologies ne sont guère efficaces. Elles peuvent avoir leur utilité en tant que complément de la législation nationale (lorsque pouvoirs publics et consommateurs déterminent que cette approche est appropriée) et lorsque les consommateurs sont sensibilisés et actifs.

Par ailleurs, les pouvoirs publics peuvent prendre des mesures constructives pour favoriser le développement et l'utilisation des technologies protectrices de la vie privée, notamment :

- Donner l'assurance aux consommateurs que les utilisateurs de ces technologies ne font pas l'objet de discrimination le cadre d'une enquête pénale ou de l'instruction d'un procès civil. En effet, on a naturellement tendance à penser qu'un consommateur utilisant, par exemple, les technologies de cryptage fort ou d'anonymisation sur son ordinateur « a quelque chose à cacher ». La législation relative à la protection des données devrait reconnaître que les consommateurs qui choisissent de recourir à ces outils peuvent simplement se protéger contre la divulgation accidentelle des informations personnelles qui les concerne, sans pour autant cacher des activités répréhensibles. Même si cet état de choses est de nature à compliquer la tâche des services chargés de faire respecter l'application des lois et de mener les enquêtes, il importe de préserver la capacité des internautes à utiliser les technologies protectrices de la vie privée.

- Reconnaître le rôle important que ces technologies peuvent jouer en aidant les consommateurs à mettre en œuvre leur propre choix en matière de protection de la vie privée dans le cadre de n'importe quelle législation régissant la protection des données ou de la vie privée. Les consommateurs susceptibles d'ignorer l'existence des technologies protectrices de la vie privée pourraient ainsi en prendre conscience.
- Les règles de protection des données devraient encourager les aux sites Web qui utilisent des technologies protectrices de la vie privée ou les mettent à la disposition de leurs clients. L'entreprise qui prend des mesures supplémentaires pour rendre le consommateur autonome, soit en lui offrant, sur son site, des choix solides, soit en intégrant des outils de confidentialité à sa propre infrastructure, devrait bénéficier d'un préjugé favorable en cas de plaintes de consommateurs ou dans des situations analogues.
- Les sites Web ne devraient pas être autorisés à exercer de discrimination à l'égard des consommateurs qui déploient des technologies protectrices de la vie privée, sauf si ce sont ces mêmes technologies qui empêchent le site de répondre aux demandes des consommateurs. Par exemple, un site ne devrait pas refuser d'afficher pour un consommateur uniquement parce que celui-ci décide de ne pas accepter de témoins de connexion. En revanche, le site devrait avoir toute latitude pour mettre en œuvre les technologies ou outils qu'il juge les mieux adaptés. Par exemple, tout comme un hôtel qui demande un numéro de carte de crédit ou des arrhes pour accepter une réservation ne saurait être tenu de garder une chambre pour un client qui refuse d'accéder à sa demande, un site Web ne pourra non plus être tenu de fournir une information individualisée ou de faciliter les cyberachats si la technologie qui y est déployée est celle des témoins de connexion et que l'internaute décide de ne pas accepter de témoins, sauf si ces derniers ont pour objet, qui vont au-delà de la personnalisation ou du marketing, de remplir un cyberchariot ou de renforcement la sécurité.

Initiatives du secteur privé

Il y a longtemps également que le secteur privé a reconnu le rôle important des technologies protectrices de la vie privée. La diversité de ces technologies démontre que les entreprises sont soucieuses de répondre aux préoccupations des consommateurs qui cherchent des moyens pour mieux contrôler la situation. Les entreprises qui utilisent l'Internet comprennent que les inquiétudes liées à la protection de la vie privée constituent un obstacle à l'expansion future du commerce électronique. Le secteur privé s'efforce d'apaiser ces inquiétudes et de lever les obstacles à la croissance future en mettant en œuvre un large éventail de technologies protectrices de la vie privée sur l'Internet et les autres réseaux pour permettre au consommateur de faire des choix éclairés en ce qui concerne la collecte et l'utilisation des informations personnelles le concernant.

Le secteur privé peut évaluer la possibilité d'utiliser plus largement ces technologies pour appuyer les objectifs des responsables de l'action gouvernementale intéressés à en étudier la viabilité pour la protection de la vie privée. En ce sens il est recommandé de poursuivre la réflexion selon les axes suivants :

- Les entreprises devraient déterminer si, en incorporant les technologies protectrices de la vie privée à leurs réseaux, elles contribueront à protéger la vie privée des utilisateurs de ces réseaux (c'est-à-dire dans l'entreprise). De même, les fournisseurs de services Internet devraient déterminer si la mise à disposition de ces technologies pourrait apaiser bon nombre des préoccupations exprimées par les abonnés en ce qui concerne la protection de la vie privée.
- Les associations de consommateurs et les organismes professionnels devraient collaborer avec les pouvoirs publics pour faire connaître aux consommateurs l'existence des technologies protectrices de la vie privée et les sensibiliser à leur utilisation.

- Les responsables des sites de commerce électronique et d'autres activités en ligne qui collectent des informations personnelles devraient déterminer si l'intégration de ces technologies, telles que la norme P3P, à leurs propres sites est possible et serait utile pour les consommateurs.
- Les entreprises de produits technologiques devraient examiner comment les technologies protectrices de la vie privée pourraient être mieux intégrées aux instruments en ligne standard, tels que les navigateurs, les logiciels clients FTP et d'autres logiciels, matériels et terminaux mobiles portatifs utilisés pour l'accès.

Conclusion

Le secteur privé et les responsables de l'action gouvernementale ont reconnu depuis longtemps l'importance que revêtent les technologies protectrices de la vie privée pour aider les consommateurs à faire des choix éclairés en matière de protection de la vie privée. L'OCDE a réaffirmé l'importance de ces technologies dans plusieurs déclarations, documents de conférence et études ces dernières années. Cette reconnaissance du rôle des technologies protectrices de la vie privée par les décideurs a avivé l'intérêt des consommateurs et des entreprises pour ces technologies et pour la poursuite de leur développement.

Le marché continuant à mettre au point de nombreux outils efficaces, il faut sensibiliser les consommateurs à leur utilité. L'industrie, les organismes du secteur privé et les pouvoirs publics peuvent les aider à se familiariser avec les technologies protectrices de la vie privée, à comprendre comment elles peuvent aider le citoyen à protéger ses données personnelles, et encourager leur utilisation. Ces efforts ne peuvent que renforcer la confiance des consommateurs et par le fait même appuyer l'expansion continue du commerce électronique, en faisant en sorte que les avantages qui s'y rattachent profitent à tous les utilisateurs du cyberespace.

NOTES

1. Selon la société de recherche britannique Arc Group, www.the-arc-group.com, le marché du fixe sans fil s'étendra rapidement au-delà de l'Europe et des États-Unis au cours des prochaines années. En 2005, le marché de l'Europe s'établira à USD 11 milliards, celui des États-Unis à 9 milliards et celui du reste du monde à USD 22 milliards.

2. Cependant, il convient de noter qu'au moins une partie des consommateurs sont d'avis qu'ils contrôlent davantage qu'auparavant l'information les concernant. Ainsi, selon le rapport annuel 1999-2000 du Commissariat à la protection de la vie privée, « En général, les Canadiens semblent moins préoccupés par leur vie privée qu'ils ne l'étaient en 1992. En 1999, 47 % des Canadiens croyaient avoir moins de vie privée au quotidien qu'ils n'en avaient il y a dix ans, par rapport à 60 % en 1992. La proportion de personnes croyant qu'il n'y a plus vraiment de vie privée parce que le gouvernement peut tout savoir sur les citoyens est passée de 81 à 63 %. La proportion de Canadiens d'accord avec un énoncé semblable concernant les entreprises est passée quant à elle de 71 à 57 %. Les résultats du sondage de 1999 laissent croire que les Canadiens ont une perception plus affinée de la notion de vie privée. 50 % des gens interrogés croient qu'ils en savent désormais suffisamment pour prévoir les impacts d'une nouvelle technologie sur le vie privée. Ils n'étaient que 43 % en 1992. La majorité des Canadiens (54 %) ne voit pas de problème à ce que les entreprises utilisent leurs renseignements personnels, du moment qu'ils le savent et qu'ils peuvent s'y opposer. La population semble prête à fournir des renseignements personnels dans certains cas et peut même vouloir sacrifier une partie de sa vie privée à condition de savoir ce dans quoi elle s'embarque. » Voir www.privcom.gc.ca/english/02 04 08 e.htm.

3. Ceci désigné généralement sous le nom « données de parcours ».

4. En général, le témoin contient l'identification de la session, qui est un code créé par le serveur. Dans certains cas, l'utilisation d'un témoin peut protéger la vie privée. Imaginons une situation où un utilisateur se connecte à un compte en ligne. Un témoin dans lequel est fixée une temporisation Web (c'est-à-dire une déconnexion automatique au bout d'une certaine période) permet d'éviter la divulgation accidentelle de données si l'utilisateur oublie de se déconnecter d'un site ou utilise un ordinateur partagé.

5. Les document RFC (« *Request for Comment* ») sont des publications de référence, notamment des descriptions de protocoles ou de normes techniques, qui sont rédigées par *l'Internet Engineering Task Force* (IETF).

6. Cette fonctionnalité est déterminée par les paramètres du navigateur Web, qui limitent les sites capables de lire de l'information de témoins en se fondant sur ces pratiques communes normalisées.

7. HTML est l'abréviation de « HyperText MarkUp Language » (langage de balisage hypertexte), qui est le langage standard utilisé pour créer des pages Web.

8. Les bloqueurs de témoins sont l'une des technologies de renforcement de protection de la vie privée qui permettent aux internautes d'exercer un plus grand contrôle sur l'installation de témoins dans leur ordinateur. Ces bloqueurs sont décrits plus précisément dans la section consacrée aux technologies protectrices de la vie privée.

9. FTP est l'abréviation de « *File Transfert Protocol* ». Le protocole FTP était l'un des premiers services offerts sur l'Internet. Il sert à partager les fichiers entre ordinateurs sur les réseaux publics. Les modules d'extension sont des applications qui donnent accès à d'autres services Web, comme le son ou la vidéo.

10. L'expression « milieux technologiques » est très générale et n'a pas de véritable définition. Dans le présent document, elle recouvre les développeurs de logiciels, les professionnels des technologies de l'information et les autres professionnels associés à la création, à la mise en œuvre et au déploiement de solutions technologiques.

11. Les données stockées dans les témoins sont en général codées, cryptées ou stockées sous une forme qui n'est pas facilement reconnaissable pour l'utilisateur. Certains ont demandé pourquoi l'information stockée ainsi dans les témoins n'est pas facile à déchiffrer. Il y a plusieurs raisons à cela. Premièrement, ces données sont en général codées de façon à limiter au minimum l'espace occupé dans les témoins et au cours des transferts de données, et à accélérer pour l'utilisateur des connexions qui sont souvent relativement lentes. Deuxièmement, des données codées ne sont pas accessibles aux autres sites Web, ce qui permet de protéger dans une certaine mesure la nature opérationnelle d'un site donnée contre des sites concurrents. Troisièmement, des données codées sont moins susceptibles d'être volées ou interceptées par un tiers qui, comme l'utilisateur, ne les comprendra vraisemblablement pas. Il est beaucoup moins probable qu'un témoin portant la mention « USER = 8323 » identifie quelqu'un qu'un témoin où figurerait « USER = AnneDupond ». Les données codées peuvent ainsi effectivement renforcer la protection de la vie privée dans les situations où des données à caractère personnel pourraient être stockées sur un témoin, car elles constituent un élément dissuasif pour quelqu'un qui serait tenté de recueillir des données stockées sur l'ordinateur d'un autre internaute. Enfin, les données codées peuvent empêcher un utilisateur d'altérer les paramètres stockés dans un témoin, ce qui assure que l'usage auquel il est destiné – par exemple enregistrer de l'information de connexion ou les préférences en vue d'une personnalisation – ne soit pas perdu accidentellement.

12. Plus la clé est longue (sa longueur étant exprimée en nombre de bits), plus le cryptage est fort. La plupart des spécialistes de la sécurité s'accordent à reconnaître qu'il faut une clé d'une longueur d'au moins 128 bits pour protéger des données. En cryptage commercial, il est courant d'utiliser des clés plus longues, et pour le cryptage personnel, on dispose maintenant d'outils permettant de créer des clés d'une longueur de 1 024 bits.

13. XML (langage de balisage extensible) est une norme définie par le W3C qui permet de définir un contexte pour les données de sites Web. HTML (langage de balisage hypertexte) est le langage utilisé pour créer des pages Web, mais il est relativement primitif dans la mesure où il ne peut contrôler que la façon dont l'information est affichée. XML peut définir ce que signifient les données dans le contexte de la page Web ou la relation qu'elles entretiennent avec d'autres données, ce qui accroît grandement la fonctionnalité d'une page Web ainsi que l'interopérabilité des données qui y sont affichées avec d'autres sites, bases de données ou applications en ligne.

14. Les pare-feu, par exemple, ont parfois la capacité de neutraliser certains services comme le FTP ou de fermer des accès spécifiques, ou encore offrent des technologies perfectionnées de détection des intrusions.

RÉFÉRENCES

National Consumers League (2000), "Online Americans More Concerned about Privacy than Health Care, Crime, and Taxes, New Survey Reveals", 4 octobre, www.nclnet.org/pressessentials.htm.

Chapitre 13

LES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE : RAPPORT SUR LE FORUM DE L'OCDE

Ce chapitre résume un forum de l'OCDE sur les technologies protectrices de la vie privée (TPVP) tenue le 8 octobre 2001. L'objectif du forum était de présenter des démonstrations d'un certain nombre de TPVP, pour permettre aux délégués d'en faire l'expérience pratique, et de faciliter des échanges de vues sur les sujets suivants : *(i)* les implications des TPVP pour l'action des pouvoirs publics et l'avenir de ces technologies dans le cadre plus large de la protection de la vie privée dans le cyberespace ; et *(ii)* les défis à relever et les méthodes à appliquer pour sensibiliser les entreprises à l'importance de la protection de la vie privée à la source ainsi que de l'utilisation des TPVP et sensibiliser les citoyens aux avantages et aux limites de ces technologies. Le résumé du forum est précédé par le document d'orientation qui fournissait aux participants des informations générales en prévision du forum, ainsi que deux études :

- Une synthèse des TPVP actuellement disponibles sur le Web ainsi qu'un tableau récapitulatif des technologies examinées. Cette étude a été remise aux participants avant le forum afin de les aider à mieux comprendre les types de produits disponibles sur le marché et leurs effets possibles sur la protection de la vie privée dans le cyberespace.

- La note de recherche de M. Perri 6 qui examine la question de savoir quand, pour qui et dans quelles circonstances les stratégies de "communication" concernant les TPVP peuvent être efficaces pour encourager les entreprises à fournir ces outils, et les citoyens à les utiliser.

Chapitre 13

LES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE : RAPPORT SUR LE FORUM DE L'OCDE

Principaux points

Le Forum a permis aux participants d'acquérir une meilleure connaissance pratique des technologies protectrices de la vie privée (TPVP), de leurs fonctionnalités et de leur utilité pour assurer la protection de la vie privée. A cet égard, la présentation de l'enquête sur 135 sites Web offrant des TPVP a donné une description plus précise des technologies disponibles aujourd'hui. Le Forum a également été l'occasion de lancer le débat sur le sujet et a permis de dégager une convergence de vues sur les diverses nouvelles questions que l'utilisation des TPVP pose aux pouvoirs publics, notamment celles qui concernent l'éducation nécessaire en la matière. Les points saillants du Forum sont récapitulés ci-après.

Les TPVP peuvent contribuer à assurer la protection de la vie privée en ligne dans le cadre d'une réglementation en bonne et due forme ou d'une autorégulation de l'industrie.

Les TPVP sont des outils technologiques qui offrent un éventail de fonctionnalités. Elles peuvent filtrer les témoins de connexion (*cookies*) et d'autres technologies de pistage, assurer l'anonymat de la navigation sur le Web et du courrier électronique, offrir une protection par cryptage des données ou permettre la gestion automatisée des données individuelles pour le compte de l'utilisateur. La plupart des TPVP disponibles aujourd'hui sont destinées aux consommateurs. Celles qui sont destinées aux organisations sont moins nombreuses, et celles qui peuvent être utilisées à la fois par les particuliers et les entreprises le sont encore moins.

Les TPVP peuvent être employées pour déterminer, par exemple, si un site contrevient à un principe donné de protection de la vie privée (ce qui permet de renforcer la transparence/notification) ou pour empêcher un site de prendre une mesure donnée sans le consentement de l'usager (renforcement de la fonction choix). C'est pourquoi, que leur utilisation s'inscrive dans un environnement d'autorégulation ou dans un cadre juridique régissant la protection de la vie privée, les TPVP peuvent garantir le respect d'au moins certains des principes fondamentaux de protection de la vie privée qui constituent les normes en la matière.

Les TPVP ont leurs avantages et leurs limites : elles font partie d'un ensemble plus large de solutions axées sur la protection de la vie privée dans le cyberespace.

Si on les évalue à l'aune des principes de protection de la vie privée retenus par l'OCDE, la plupart des TPVP actuelles destinées aux particuliers permettent de limiter la collecte de données ou de laisser à la personne concernée le choix à cet égard (45 %), d'éviter la collecte de données (40 %) et d'assurer la sécurité des données (27 %). Cependant, aucune des technologies disponibles n'assure une protection totale de la vie privée qui soit conforme aux Lignes directrices de l'OCDE : la plupart des technologies examinées ne permettent d'appliquer que l'un des principes retenus par l'OCDE, et une seule d'entre elles en intègre cinq.

Les TPVP destinées aux entreprises peuvent automatiquement suivre et analyser la collecte et l'utilisation de l'information, ainsi que les éventuelles pratiques en matière de partage. Elles peuvent ainsi aider les entreprises à se conformer à leur propre politique de protection de la vie privée. Cependant, pour qu'elles trouvent toute leur utilité pour les entreprises, les TPVP devraient être intégrées à un programme de gestion des risques d'atteinte à la vie privée.

Les TPVP s'inscrivent donc nécessairement dans le cadre plus vaste de la protection de la vie privée en ligne qui comprend des dispositions réglementaires et des mécanismes d'autorégulation ainsi que d'autres initiatives telles que la formulation et la notification de politiques de protection de la vie privée, l'utilisation de solutions contractuelles et l'accessibilité croissante des mécanismes de règlement des différends en ligne comme recours possible.

Une plus grande transparence et une meilleure utilisabilité des TPVP pourraient renforcer la confiance des utilisateurs/consommateurs.

Les statistiques actuelles indiquent que les utilisateurs et consommateurs éprouvent encore quelque réticence à s'engager dans des transactions de commerce électronique ou d'autres activités en ligne qui nécessitent la communication de données à caractère personnel. Les TPVP offrent une solution partielle à ce problème, mais encore faut-il qu'elles inspirent aux utilisateurs une solide confiance dans leur capacité à protéger la vie privée.

L'une des limites de certaines TPVP tient à ce que les utilisateurs ne disposent pas d'une information complète sur l'organisation sous-jacente ou sur d'autres caractéristiques. Autre limite, ces technologies sont parfois de nature technique et ne sont pas suffisamment simples pour être utilisées par le consommateur moyen. Pour être plus efficaces et plus largement utilisées, et ainsi contribuer au renforcement de la confiance dans le cyberespace, les TPVP doivent donc devenir plus transparentes et plus faciles à utiliser.

Le point de départ – sensibiliser les entreprises et les particuliers.

Il est très important de sensibiliser les entreprises et les citoyens à l'existence des TPVP et de les aider à comprendre les avantages et les limites de ces technologies ainsi que le rôle complémentaire qui leur incombe dans le cadre de la protection de la vie privée. Diverses stratégies d'éducation seront nécessaires pour adapter ces initiatives aux différents groupes visés afin de promouvoir efficacement l'utilisation des TPVP et d'en optimiser les avantages.

S'agissant des entreprises, il faut leur rappeler à quel point il importe de gérer les risques d'atteinte à la vie privée ou à la sécurité et les inciter à équilibrer leurs coûts, de sorte que la protection de la vie privée soit prise en compte d'emblée et que la charge qui lui est associée ne pèse pas lourdement sur le consommateur. Les entreprises peuvent être encouragées dans cette voie par des stratégies ciblées visant à leur faire prendre conscience de l'importance que revêt la protection de la vie privée pour renforcer la confiance des clients et établir des relations mutuellement avantageuses. Elles auront ainsi la motivation nécessaire pour mieux informer les consommateurs de leurs pratiques en matière de protection de la vie privée, et leur assurer la confidentialité voulue pendant les transactions et les entretiens en ligne. Il doit également être rappelé aux entreprises combien il importe d'intégrer les TPVP à la conception des nouveaux produits.

S'agissant des particuliers, il est de toute évidence nécessaire de les sensibiliser mieux et davantage pour les encourager encore à tirer parti des TPVP lorsqu'ils naviguent sur le Web, expédient ou reçoivent des courriers ou s'engagent dans d'autres activités électroniques. Étant donné la nature technique de ces

produits, une tâche particulière consistera à expliquer ces technologies en langage simple, étant donné leur complexité par rapport au niveau général de compréhension de la population. Cependant, les utilisateurs et les consommateurs n'auront confiance dans ces technologies que s'ils comprennent comment elles fonctionnent, comment elles sont mises en œuvre et quels en sont les avantages et les limites pour répondre à leurs exigences en matière de protection de la vie privée.

I. Présentation du forum : document d'orientation et aperçu du programme

Introduction

Dans la déclaration des Ministres relative à la protection de la vie privée sur les réseaux mondiaux, formulée à Ottawa en 1998, les gouvernements des pays membres de l'OCDE ont pris l'engagement de « garantir la mise en œuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée en ce qui concerne les réseaux mondiaux » (OCDE, 1980). Cet engagement portait notamment sur cinq mesures, dont l'une consistait à encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée.

Au cours des trois années écoulées depuis la Conférence d'Ottawa et la déclaration ministérielle, le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) a concentré sa réflexion sur la mise en œuvre d'autres éléments de ce programme en cinq volets, notamment sur les solutions contractuelles, les mécanismes alternatifs de règlement des litiges, le lancement du générateur de déclaration de politique de protection de la vie privée de l'OCDE (qui a pour but de favoriser l'adoption de politiques de protection de la vie privée et la notification de ces politiques aux utilisateurs) ainsi que sur d'autres actions menées pour sensibiliser les utilisateurs, les entreprises et les pouvoirs publics aux questions concernant la protection de la vie privée en ligne. Pendant cette même période, des progrès notables ont été réalisés dans l'élaboration et l'utilisation de technologies protectrices de la vie privée (TPVP). De nombreux responsables de l'action gouvernementale misent beaucoup sur la capacité de ces technologies à faciliter l'application de principes de protection de la vie privée, tels que ceux qui sont énoncés dans les Lignes directrices de l'OCDE, dans le cadre d'une autorégulation par l'industrie ou d'une réglementation classique.

A la réunion de février 2001 du GTSIVP, les délégués ont entendu un exposé de Wendy Lader (ministère du Commerce des États-Unis) sur un atelier que le gouvernement des États-Unis avait consacré aux TPVP[1], ainsi qu'un exposé de Lauren Hall (*Software and Information Industry Association* et consultant auprès du Secrétariat de l'OCDE) sur un inventaire de ces technologies établi pour le GTSIVP[2]. Le Groupe de travail a procédé à un échange de vues sur le sujet et décidé que le moment était venu d'examiner de façon plus approfondie les grandes questions liées à ces nouvelles technologies. Les délégués sont convenus de la nécessité de sensibiliser le public à l'existence des TPVP et de faciliter l'initiation à leur utilisation, estimant que celle-ci peut compléter les politiques de protection de la vie privée, en donnant, par exemple, aux utilisateurs les moyens de choisir les entreprises dont les pratiques en matière de protection de la vie privée correspondent le mieux à leurs préférences.

Il a également été décidé de tenir un forum spécial sur les TPVP, auquel seraient également conviés les délégués du Comité de la politique à l'égard des consommateurs et des représentants des associations de consommateurs, et au cours duquel seraient présentées des démonstrations d'un certain nombre de technologies. Les participants auraient l'occasion de faire eux-mêmes l'expérience de l'utilisation de ces technologies et d'échanger leurs vues sur les sujets suivants :

- Les implications des TPVP pour l'action des pouvoirs publics, et l'avenir de ces technologies et de la protection de la vie privée dans le cyberespace en général.

- Les défis à relever et les méthodes à appliquer pour sensibiliser les entreprises à l'importance de l'intégration de la protection de la vie privée à la conception des produits, ainsi qu'à l'utilisation des TPVP. et
- Les défis à relever et les méthodes à appliquer pour sensibiliser les citoyens aux avantages et aux limites de ces technologies.

La synthèse ci-après des questions qui se posent aux pouvoirs publics en ce qui concerne les TPVP avait pour but de fournir aux délégués des informations et des éléments de réflexion avant le Forum. Pour un examen plus approfondi de certaines de ces technologies et de leur fonctionnement, il était conseillé aux participants de consulter la documentation répertoriée plus loin, dans la section intitulée « Autres sources d'information ».

Panorama des technologies protectrices de la vie privée

Les technologies protectrices de la vie privée ainsi que leurs finalités ont fait l'objet de diverses définitions :

- Lauren Hall, dans son inventaire, attribue comme objectif aux TPVP de permettre à l'utilisateur ou au responsable de la technologie dans une entreprise de contrôler la divulgation d'information, la quantité d'information divulguée et les conditions dans lesquelles elle est divulguée et/ou traitée[3].
- Le Groupe de travail sur la protection des données (article 29) de la Commission européenne note que le concept de TPVP « concerne une gamme de technologies qui assurent la protection de la vie privée, notamment en minimisant ou en éliminant la récolte de données identifiables » (UE, 2000).
- Selon Herbert Burkert, du *German Institute for Media Communication*, le terme désigne les concepts techniques et organisationnels qui concernent la protection de l'identité (Burkert, 1997)[4].
- Le Commissaire à l'information et à la vie privée de l'Ontario et le *Registratiekamer* des Pays-Bas, dans leur étude conjointe, insistent sur le rôle des TPVP comme « protecteur d'identité » (Commissaire à l'information et à la vie privée de l'Ontario et *Registratiekamer*, 1995).

Autrement dit, les TPVP sont des outils technologiques qui aident à assurer le respect de la vie privée des internautes/consommateurs. Elles sont le plus souvent considérées dans le cadre de l'action gouvernementale comme s'inscrivant dans un ensemble plus large de mesures axées sur la protection de la vie privée. Étant donné leur finalité, il n'est pas étonnant que ces technologies, telles qu'elles se présentent actuellement ou sont imaginées, puissent avoir des caractéristiques très diverses. Certaines filtrent les témoins de connexion (*cookies*) et d'autres agents de traçage, d'autres assurent l'anonymat de la navigation sur le Web et du courrier électronique. Il en existe qui offre une protection par cryptage des données tandis que d'autres visent essentiellement à assurer la confidentialité et la sécurité des achats effectués par voie électronique. Certaines enfin permettent la gestion automatisée des données individuelles des usagers pour le compte de ceux-ci.

La liste pourrait certes être beaucoup plus longue. Le prodigieux essor de l'utilisation de l'Internet et du cybercommerce s'est accompagné d'une explosion correspondante des technologies de la confidentialité et de la sécurité que l'on regroupe sous le terme « technologies de protection de la vie privée » (TPVP). Cet « espace de vie privée » dans l'économie est devenu un enjeu concurrentiel, et nombreuses sont les sociétés qui souhaitent attirer l'intérêt des usagers, des autres entreprises et des

pouvoirs publics. Cet afflux d'entreprises spécialisées en protection de la vie privée et en sécurité naît alors même que des enquêtes continuent de démontrer que les internautes éprouvent quelque inquiétude au sujet de leur vie privée lorsqu'ils s'aventurent dans le cyberespace et en particulier lorsqu'ils y effectuent des achats pour lesquels ils doivent souvent révéler des renseignements à caractère personnel[5]. Il y a également lieu de croire que les citoyens souhaitent être plus amplement informés des pratiques en matière de respect de la vie privée qui ont cours dans les entreprises et organismes avec lesquels ils effectuent des transactions[6].

Les avantages des TPVP

Les partisans du développement des TPVP sont issus de l'industrie, des organismes voués à la protection de la vie privée ainsi que de nombreux organismes publics des pays de l'OCDE. Ils font souvent valoir deux avantages solides que ces technologies offrent aux décideurs dans le monde. D'abord, elles peuvent aider à mettre en pratique certains des principes de protection de la vie privée qui sont reconnus internationalement. Ensuite, elles peuvent autant être utilisée par les pays qui ont opté pour un cadre d'autorégulation et par ceux qui mise sur une réglementation classique de la protection de la vie privée.

Tableau 13.1. **Les TPVP et les principes de protection de la vie privée**

Exemples de types courants de TPVP	Exemples des principaux effets *(en fonction des Lignes directrices de l'OCDE sur la protection de la vie privée)*
Outils d'anonymisation/pseudonymisation	Limitation de la collecte (ou évitement de la collecte)
Outils de gestion des données à caractère personnel (par exemple, courtiers en information et infomédiaires)	Limitation de la collecte ; sécurité
Outils de notification/choix (par exemple, P3P)	Transparence/notification ; limitation de la collecte/consentement et choix
Outils de contrôle du marketing/publicité (par exemple, filtres de témoins de connexion, détecteurs de logiciels espions et outils de gestion du consentement-marketing)	Limitation de la collecte ; choix et/ou consentement ; sécurité
Outils de sécurisation	Sécurité
Outils de protection de la vie privée/sécurisation pour le commerce électronique	Limitation de la collecte ; sécurité
Outils de contrôle d'accès	Notification ; sécurité ; limitation de l'utilisation ; accès de la personne concernée
Outils de protection de la vie privée des enfants	Limitation de la collecte/consentement
Outils d'audit/vérification de conformité aux normes de protection de la vie privée	Responsabilité

Source: OCDE.

Les TPVP permettent à l'internaute de déterminer, par exemple, si un site contrevient à un principe donné de protection de la vie privée (d'où renforcement au plan de la transparence/notification) ou d'empêcher un site d'engager une action donnée sans son consentement (renforcement de la possibilité d'exercer un choix).

Motifs d'inquiétude et limites

Il apparaît toutefois clairement que toutes les TPVP ne font pas l'unanimité chez les défenseurs de la vie privée. D'aucuns jugent certaines technologies trop faibles, voire trompeuses et de nature à affaiblir plutôt qu'à renforcer la protection de la vie privée, ou les considèrent encore comme un leurre empêchant la mise en place d'une éventuelle réglementation protectrice de la vie privée. Le projet P3P, très populaire

dans l'industrie et auquel souscrivent de nombreux groupes de protection de la vie privée, a été critiqué par certains. *Consumers International*, par exemple, a affirmé dans son étude Privacy@net 2001 que certaines technologies, notamment la norme P3P, visaient davantage à faciliter la mise en commun de données qu'à protéger les usagers[7].

Les partisans des TPVP ont écarté bon nombre de ces critiques. Le Centre indépendant du Schleswig-Holstein pour la protection de la vie privée (Allemagne), par exemple, a fait part de son entière adhésion à la norme P3P, notant qu'elle permet aux usagers d'exercer davantage de contrôle sur ce qu'il advient de leurs données à caractère personnel[8]. Malgré tout, la plupart de ceux qui militent en faveur des diverses TPVP (y compris le Centre indépendant pour la protection de la vie privée) se refuseraient aujourd'hui à affirmer qu'elles peuvent dissiper toutes les inquiétudes concernant la protection de la vie privée dans le cyberespace.

Quelques exemples des limites des TPVP le démontrent. D'abord, bon nombre d'entre elles protègent la vie privée des particuliers pendant qu'ils sont en ligne, servent à les prévenir ou à obtenir leur consentement le cas échéant, mais elles ne peuvent garantir la confidentialité de l'information une fois que celle-ci a été communiquée à une organisation ou entreprise. La nécessité de veiller à ce que l'information collectée soit traitée conformément aux principes de protection de la vie privée (tels que celui de la limitation de l'utilisation, énoncé dans les Lignes directrices de l'OCDE) constitue par conséquent un important motif de préoccupation. Dans le même temps, la possibilité de se soustraire totalement à la collecte de données grâce aux outils d'anonymisation soulève également des questions quant à l'absence de responsabilité dans le cyberespace et peut être préoccupante pour les services chargés de faire respecter les lois et règlements.

Le débat n'est pas clos non plus sur les paramètres implicites des TPVP. L'hypothèse selon laquelle bon nombre de consommateurs, voire la plupart, ne modifieront ou ne personnaliseront pas les paramètres prédéfinis de leur technologie protectrice confère à ces derniers une importance accrue, surtout dans le cadre d'un débat sur la protection de la vie privée. Si un usager ne modifie pas, par exemple, les paramètres de son filtre de témoins de connexion, le nombre de témoins qui seront bloqués, leur type et la nature de l'information communiquée à l'usager au sujet des témoins qui seront installés sur son ordinateur seront déterminés par le préréglage du filtre. C'est pourquoi certains craignent que les paramètres prédéfinis de certaines technologies ne soient pas suffisamment rigoureux pour assurer une protection véritablement renforcée de la vie privée de leurs utilisateurs. (Inversement, d'autres font valoir que des paramètres trop stricts, qui bloqueraient, par exemple, tous les types de témoins de connexion, risquent d'entraver exagérément des activités telles que la navigation sur le Web.)

Par ailleurs, les TPVP suscitent des préoccupations d'ordre pratique, notamment la question de savoir si elles sont suffisamment simples pour être utilisées par le consommateur moyen et si ce dernier est prêt à se les procurer, à les installer et à les utiliser sur son ordinateur. On se demande également si le nombre d'utilisateurs de TPVP augmentera au point d'atteindre une masse critique qui obligera les opérateurs de sites Web à modifier leurs pratiques en matière de protection de la vie privée, ou si ce sont, au contraire, les utilisateurs de ces technologies qui seront obligés de renoncer à une certain degré de performance sur le Web au nom de la protection de la vie privée. Les entreprises, quant à elles, pourraient bien nourrir une certaine appréhension devant la complexité du processus d'intégration des outils de protection de la vie privée à leurs activités et/ou produits.

De simples outils

Ces limites et préoccupations étant prises en compte, il demeure que les avantages propres aux TPVP assurent à ces dernières une place dans la panoplie de mesures qui seront mises en œuvre pour protéger la vie privée dans le cyberespace à l'avenir, comme le préconise la Déclaration ministérielle de 1998. Cependant, il importe de ne pas perdre de vue que ces technologies sont de simples outils, destinés à être utilisés par les citoyens, les entreprises ou les pouvoirs publics. C'est dans une large mesure les décisions qui seront prises par leurs utilisateurs, et non les outils en eux-mêmes, qui détermineront s'ils sont mis en œuvre de façon positive ou négative, constructive ou obstructive. (Comme l'écrit Burkert, « il ne faut pas oublier que les TPVP relèvent essentiellement du domaine technique : cela veut dire qu'elles *suivent* une décision normative », Burkert, 1997.) Dans le même temps, on prendra également soin de noter la très grande diversité de ce que l'on entend par « TPVP ». Toutes ne seront pas aussi efficaces ou rigoureuses qu'on pourrait le souhaiter. Certaines pourront même être aussi nocives ou intrusives qu'on pourrait le craindre. Elles ne déclencheront peut-être pas toutes non plus d'opposition à leur utilisation, pas plus qu'elles ne susciteront forcément d'arguments en leur faveur.

Une éducation à faire

Les TPVP étant des outils, qui comportent à la fois d'importants avantages et des limites pour les utilisateurs et les entreprises, une initiation à ces outils s'impose. C'est ce que soutient le sociologue Gary Marx en ce qui concerne les implications des technologies de l'information en général pour la protection de la vie privée, faisant observer « qu'il importe que la technologie soit démystifiée et que les utilisateur n'y attribuent pas des vertus qu'elle ne possède pas. Le 'mythe de la surveillance' présente un redoutable danger lorsqu'on exagère le pouvoir des technologies de l'information. Par ailleurs, lorsque les technologies se révèlent moins performantes que ce que les autorités prétendent, c'est la légitimité qui en souffre. Il importe donc de comprendre le potentiel et les limites de la technologie » (Marx, 1990).

S'agissant de démystifier les TPVP et d'en promouvoir l'utilisation en vue d'en optimiser les avantages, les efforts de sensibilisation doivent être déployés au moins dans trois directions. Ils doivent d'abord s'adresser aux utilisateurs individuels, qui souhaiteront peut-être tirer parti de ces technologies lorsqu'ils naviguent sur le Web, envoient ou reçoivent du courrier électronique ou participent à des activités dans le cyberespace. Des efforts doivent aussi être orientés vers les entreprises, pour les inciter à utiliser des technologies pouvant les aider à maintenir la confidentialité des ventes en ligne, à mieux informer les consommateurs de leurs pratiques en matière de protection de la vie privée et/ou à améliorer les mécanismes de contrôle de l'accès à leurs bases de données. Enfin, il importe d'encourager les entreprises à intégrer des TPVP à la conception des nouveaux produits.

Les actions de sensibilisation devront par conséquent être modulées en fonction des différents publics et cadres d'utilisation. Dans tous les cas, il faudra s'attacher à faire comprendre les solutions qu'offrent les TPVP, mais aussi les limites qui les empêchent de répondre à la totalité des besoins en la matière.

Selon une récente enquête réalisée par Harris Interactive pour la *Privacy Leadership Initiative*, rares sont les internautes qui exploitent actuellement les possibilités des TPVP[9]. A peine 15 % d'entre eux déclarent avoir installé un logiciel sur leur ordinateur pour protéger leurs données à caractère personnel, tandis que seulement 10 % utilisent un logiciel d'anonymisation de leur navigation dans le cyberespace et 5 % ont déclaré utiliser des logiciels d'anonymisation des achats. (Les chiffres sont quelque peu supérieurs pour les internautes assidus et inférieurs pour les internautes occasionnels.)

Autres sources d'information

Récents ateliers et rapports

- Atelier du *Department of Commerce* des États-Unis (septembre 2000) : www.ntia.doc.gov/ntiahome/privacy/
- Atelier du *Joint Research Centre* (CE) (mai 2000) : http://dsa-isis.jrc.it/Privacy/
- Groupe de travail sur la protection des données – Article 29 de l'UE, document de travail, « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne » (novembre 2000). Une section y est consacrée aux TPVP : http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf

Panorama des TPVP

- Panorama des outils de protection de la vie privée, par Lorrie Faith Cranor, AT&T Labs (septembre 2000) : www.research.att.com/~lorrie/pubs/privacy-tools-sept2000.html
- « The Reinvention of Privacy par Toby Lester in *The Atlantic Monthly* (mars 2001) : www.theatlantic.com/issues/2001/03/lester-p1.htm
- « Networking Health: Prescriptions for the Internet », Conseil national de recherche (2000). On y trouve une analyse des technologies protectrices de la vie privée dans l'optique des questions de santé (pages 167-174, en particulier) : www.nap.edu/books/0309068436/html/

P3P (avec mention d'autres technologies)

- Sélection de documents consacrés à la technologie P3P : www.w3.org/P3P/
- Analyse de la norme P3P par le *Center for Democracy and Technology* et le Commissaire à l'information et à la vie privée de l'Ontario (mars 2000) : www.cdt.org/privacy/pet/p3pprivacy.shtml
- « Pretty Poor Privacy », rapport du *Electronic Privacy Information Center* et Junkbusters (juin 2000) : www.epic.org/Reports/prettypoorprivacy.html

Guides sur les TPVP établis par des groupes de défense de la vie privée

- *Center for Democracy and Technology :* www.cdt.org/privacy/pet/
- *Electronic Privacy Information Center :* www.epic.org/privacy/tools.html

Récente étude internationale sur la protection de la vie privée sur l'Internet

- Rapport de *Consumers International* sur la protection de la vie privée sur l'Internet, qui contient un appendice où sont examinées les TPVP (janvier 2001) : www.consumersinternational.org/news/pressreleases/fprivreport.pdf

Aperçu du programme du Forum

ACCUEIL ET PRÉSENTATION

Accueil et remarques liminaires, *Président du GTSIVP et Secrétariat*

SESSION DU MATIN: PRÉSENTATION DE LA TECHNOLOGIE

Produits des TPVP : présentations introductives

Aperçu général des TPVP disponibles sur Internet – *Laurent Bernat, Directeur de Projetweb, consultant.*

Présentation de produits TPVP destinés aux particuliers :
incidence de la limitation de la collecte/de l'évitement.

Laurent Bernat, Directeur de ProjetWeb, consultant
@nonymouse (@nonymouse.com) – (outil d'anonymisation ou de pseudonymisation).
The Cloak (the-cloak.com) – (outil d'anonymisation ou de pseudonymisation)
Privacy Companion (idcide.com) – (filtrage de témoins de connexion).
Netscape 6.1 (AOL-Netscape) – (filtrage de témoins de connexion et gestion des mots de passe)

Présentation de produits TPVP destinés aux particuliers et aux entreprises :
Incidence de la notification/transparence, de la limitation de la collecte, du consentement et du choix

P3P (World Wide Web Consortium) – (pour les serveurs)
Helena Lindskog, Responsable systèmes, Ericsson Infotech

Internet Explorer 6 (Microsoft) – (pour les clients)
Isabelle Valet-Harper, Responsable normes européennes, Microsoft Europe

Présentation de produits TPVP destinés aux entreprises: incidence de la responsabilité

WebCPO (watchfire.com) – (outil d'audit/contrôle du respect de la vie privée)
Norman McConkey, Directeur, Watchfire Ltd.

Prise en main des produits présentés

A ce stade, les participants ont été invités à se répartir en petits groupes pour faire l'expérience, sur des ordinateurs mis à leur disposition par l'OCDE, de l'utilisation des TPVP destinées aux particuliers qui leur avaient été présentées. Ils pouvaient s'adresser aux représentants des entreprises dont ils utilisaient les produits, ainsi qu'à des agents de l'OCDE, pour obtenir de l'aide au besoin. Les participants ont également été encouragés à poser des questions et à débattre entre eux.

Débat général, questions-réponses

SESSION DE L'APRÈS-MIDI : ÉDUQUER LES UTILISATEURS/CONSOMMATEURS ET LES ENTREPRISES

Perception des risques pour la vie privée et éducation à l'égard des TPVP
Perri 6, Directeur, Policy Programme de l'Institute for Applied Health and Social Policy, King's College (Londres)

« Privacy-by-design » : Protection de la vie privée à la source
Stephanie Perrin, Chef du service « Protection de la vie privée », Zeroknowledge

Éduquer les consommateurs en matière de TPVP
Naja Felter, Chargée de mission, Commerce et cybercommerce, Consumers International

Débat général et remarques de conclusion

Remarques de conclusion et aperçu du débat d'orientation du GTSIVP, *Président du GTSIVP, Secrétariat*

II. Rapport sur le forum

Accueil et présentation

Le Forum a été ouvert par M. Peter Ford, Président du Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) de l'OCDE. M. Ford a souhaité la bienvenue aux participants, et a rappelé que les Ministres des pays de l'OCDE, dans leur déclaration de 1998, avaient jugé que la technologie, en particulier les technologies protectrices de la vie privée (TPVP), constituaient un élément important de la panoplie de mesures nécessaires pour assurer la protection de la vie privée dans le cyberespace, et que le GTSIVP s'était penché sur ces technologies dans cette optique.

L'exposé liminaire a été prononcé par Mme Anne Carblanc, du Secrétariat de l'OCDE. Mme Carblanc a donné un bref aperçu de chacun des exposés qui allaient être donnés au cours du Forum ainsi que du déroulement de la rencontre. Elle a ensuite décrit dans les grandes lignes les TPVP comme des « outils contribuant à la protection de la vie privée » et a souligné que dans le contexte de l'action des pouvoirs publics, ces technologies semblaient faire partie de l'ensemble de solutions nécessaires pour assurer une protection efficace de la vie privée en ligne. Mme Carblanc a ensuite évoqué les objectifs plus larges du Forum et des travaux du GTSIVP en ce qui concerne les TPVP en général, à savoir :

- D'une part, mettre en évidence les avantages et les limites de ces technologies ainsi que les circonstances dans lesquelles leur développement et leur utilisation doivent être appuyés au niveau de l'action gouvernementale.
- D'autre part, examiner comment sensibiliser au mieux les consommateurs et les entreprises aux TPVP ainsi qu'à leur rôle dans le cadre général de la protection de la vie privée, afin de favoriser l'offre et la demande de ces outils dans l'intérêt de la protection de la vie privée dans le cyberespace.

Session I: Présentation de la technologie

Cette session avait essentiellement pour but de permettre aux participants de mieux comprendre en situation concrète ce que sont les TPVP aujourd'hui. Des démonstrations ont donné un aperçu de certaines technologies représentatives destinées soit aux particuliers, soit aux entreprises. Les participants ont ensuite été invités à utiliser par petits groupes, sur des ordinateurs fournis par l'OCDE, les technologies destinées à l'utilisateur individuel. Des représentants des organisations dont les technologies étaient utilisées, ainsi que des agents de l'OCDE, étaient présents pour leur prêter assistance le cas échéant.

Produits des TPVP : présentations introductives

Aperçu général des TPVP disponibles sur le Web

Laurent Bernat, Directeur de Projetweb, a exposé les grandes lignes d'une *Étude des technologies protectrices de la vie privée* (voir appendice I) qu'il avait réalisée en qualité de consultant auprès de l'OCDE. M. Bernat a expliqué que cette étude avait pour but de recenser les TPVP utilisées sur l'Internet et de montrer leur incidence sur la protection de la vie privée à la lumière des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel.

M. Bernat a expliqué que plus de 130 sites avaient été visités au cours de l'étude et que 83 d'entre eux avaient été retenus pour un complément d'analyse. Il a souligné que les TPVP analysées avaient été choisies sur la base de leurs fonctionnalités et a précisé que cette étude n'avait aucune vocation exhaustive, car elle ne portait pas sur les outils de cryptographie purs, les outils orientés vers la protection des enfants,

les outils d'effacement, les outils destinés à assurer la sécurité réseau du PC ou les outils de sécurisation d'accès préservant l'anonymat.

Les résultats de cette étude indiquent que les TPVP disponibles aujourd'hui offrent un éventail de fonctionnalités et que plusieurs d'entre elles en offrent plus d'une. La plupart sont des filtres de témoins de connexion (la moitié environ), les anonymiseurs sont présents dans 36 % des TPVP, tandis que les parts respectives des logiciels de cryptage, des filtres de publicité et des logiciels de confidentialité de mél se situent à un peu moins de 20 % chacune. En outre, l'étude a révélé que 80 % des TPVP examinées étaient destinées aux personnes physiques, 20 % aux personnes morales et 3 % aux deux catégories.

Par rapport aux Principes de protection de la vie privée énoncés dans les Lignes directrices de l'OCDE, l'étude montre que les TPVP d'aujourd'hui permettent pour la plupart la limitation de la collecte des données et le choix à cet égard (45%), l'empêchement de la collecte de données (40 %) et la sécurité (27 %). En outre, sur les 83 sites examinés, 58 TPVP ne concernent qu'un des huit principes retenus par l'OCDE, 44 en concernent deux, deux en concernent trois et seulement un en concerne cinq.

L'auteur de l'étude a dégagé de ces résultats un certain nombre de conclusions générales et d'autres observations, qui se résument ainsi :

- Sur le plan technique aucun des outils identifiés n'exploite un panel de fonctionnalités complet permettant de protéger totalement la vie privée des personnes. Les utilisateurs doivent par conséquent combiner plusieurs outils pour optimiser leur niveau de protection.
- Parmi les outils examinés, 51 % doivent être installés sur l'ordinateur de l'internaute, ce qui pourrait être un obstacle à leur adoption et poser des problèmes de compatibilité.
- Certains sites présentent très peu d'informations sur l'organisation qui est responsable du produit TPVP en question, sur son identité et sur ses coordonnées, ce qui peut être un frein psychologique à l'adoption des TPVP.
- De nombreux sites dénotent un réel effort pour sensibiliser les utilisateurs. Cependant, certains sites privilégient l'information commerciale plutôt que l'information technique à caractère pédagogique.

M. Bernat a conclu que les TPVP pouvaient être utiles pour aider les internautes à protéger leur vie privée mais qu'elles étaient complémentaires d'autres outils ou dispositifs. Il a souligné que pour que les utilisateurs aient confiance dans les TPVP, ils devaient comprendre la technologie et ses modalités de mise en œuvre, et savoir qui la mettait à leur disposition. M. Bernat a fait remarquer que l'éducation des consommateurs sera essentielle pour renforcer leur confiance et faire progresser l'utilisation de ces technologies. Enfin, il a mentionné un certain nombre de pistes pour des travaux ultérieurs.

Démonstration des produits TPVP destinés aux personnes physiques

M. Bernat a donné une démonstration en direct de quelques technologies destinées aux personnes physiques : deux anonymiseurs – @*nonymouse* et *The Cloak* –, et deux filtres de témoins de connexion (*cookies*) – *The Privacy Companion* et *Netscape 6.1*. En même temps, M. Bernat en a expliqué les fonctionnalités de base aux participants.

- @*nonymouse* est une interface qui permet à l'internaute de conserver l'anonymat pendant qu'il navigue sur le Web, qu'il envoie des méls et qu'il participe à des groupes de discussion.

- *The Cloak* est une interface de navigation anonyme sur le Web. En outre, grâce à une fonction de cryptage facultatif (https), il offre aux utilisateurs connectés à l'Internet par l'intermédiaire d'un réseau local un plus grand degré d'anonymat à l'égard de l'administrateur du réseau.
- *The Privacy Companion* est un outil qui est installé sur l'ordinateur de l'internaute pour filtrer les témoins de connexion. Il est efficace et convivial. Il fait la distinction entre les témoins provenant du site visité et ceux provenant de sites tiers (réseau de pistage).
- *Netscape Navigator 6.1* permet à l'utilisateur de choisir ses préférences implicites en ce qui concerne la gestion des témoins de connexion par site. Il permet également de filtrer les témoins provenant de sites tiers.

Démonstration de produits TPVP destinés à la fois aux particuliers et aux entreprises

Mme Helena Lindskog a donné un exposé sur le protocole *Platform for Privacy Preferences (P3P)* mis au point par le *World Wide Web Consortium,* côté serveur. Mme Lindskog est responsable systèmes chez Ericcson Infotech, chargée de conférences à l'université de Karstad et représentante d'Ericsson au sein du Groupe de travail P3P Initiative du *World Wide Web Consortium*.

Mme Lindskog a d'abord parlé du concept général de « vie privée » et a noté que la protection de la vie privée pouvait être améliorée par plusieurs moyens – l'anonymat, le pseudonymat, l'impossibilité d'établir un lien, l'inobservabilité, le consentement de l'utilisateur ou la législation.

Mme Lindskog a ensuite décrit le protocole P3P. Elle a expliqué que ce protocole, à son niveau de base, était une technologie qui traduisait la politique de la protection de la vie privée d'un site Web en format lisible par machine pour permettre aux navigateurs et aux autres dispositifs de lire la politique et de la comparer aux préférences du consommateur en matière de protection de la vie privée. Mme Lindskog a également présenté les étapes qu'un fournisseur de services devait suivre pour mettre en œuvre ce protocole, à savoir : *i)* élaborer une politique écrite de protection de la vie privée (le document intitulé « P3P Guiding Principles » peut être utile à cette fin) ; *ii)* décider quelle politique s'applique à quelles parties de leur site Web ; *iii)* choisir un générateur ; *iv)* saisir l'information nécessaire dans le générateur P3P; *v)* créer un fichier référence de cette politique et le stocker en un lieu spécifique ; et *vi)* utiliser le validateur P3P pour vérifier si des erreurs ont été commises.

Au cours de sa description des avantages et des inconvénients du protocole, Mme Lindskog a fait valoir que le protocole s'acquittait bien de la tâche pour laquelle il avait été conçu, c'est-à-dire fournir aux internautes un moyen de consentir à ce que leurs données soient utilisées par un site Web ou de refuser.

Mme Isabelle Valet-Harper, responsable du service « Normes européennes » de Microsoft Europe, a donné un aperçu du fonctionnement du protocole P3P du point de vue du client en utilisant le navigateur Internet Explorer 6.

Mme Valet-Harper a d'abord donné une description générale du contexte de la protection de la vie privée et de la place qu'y occupait le protocole P3P du point de vue de l'utilisateur. Elle a expliqué que ce protocole permettait à l'internaute de faire en sorte que son agent (le navigateur) agisse directement en son nom, ou lui facilite la prise de décisions en ce qui concerne ses préférences en matière de protection de la vie privée. Elle a cependant noté que le protocole P3P ne constituait qu'une partie de la solution, dans la mesure où il aide les utilisateurs à comprendre les politiques de protection de la vie privée mais que d'autres éléments – notamment les programmes et réglementations concernant les labels de confiance, les anonymiseurs, les outils de cryptage, ainsi que les lois et codes de pratique – avaient également un rôle important à jouer.

Mme Valet-Harper a ensuite parlé de façon détaillée du navigateur Internet Explorer 6 et de sa mise en œuvre du protocole P3P. Elle a fait remarquer que l'objectif de Microsoft, dans la mise en œuvre de cette technologie, consistait à aider l'utilisateur final à communiquer ses préférences en matière de protection de la vie privée de façon non obstructive. Elle a insisté sur le fait que Microsoft avait voulu fournir davantage de renseignements sur les témoins de connexion et les choix de l'internaute à cet égard, en créant un comportement automatisé plus intelligent et en offrant la possibilité de trier les témoins en fonction de leur objet.

Mme Valet-Harper a ensuite donné une démonstration du navigateur Internet Explorer 6. Elle a expliqué qu'un icône de situation apparaissait chaque fois qu'un témoin était soumis à restriction d'après les paramètres de protection de la vie privée de l'internaute. Autrement dit, lorsque le site visité utilise des témoins et que la politique de protection de la vie privée du site ne correspond pas aux critères de l'internaute, les témoins sont bloqués et l'internaute prévenu. Ce dernier peut fixer ses paramètres de confidentialité sur un « onglet-curseur » et choisir parmi six niveaux de protection – accepter tous les témoins ; protection basse ; protection moyenne ; protection moyennement haute ; protection haute ; bloquer tous les témoins – ou laisser en place les paramètres par défaut. Lorsque l'icône apparaît, l'internaute peut également double-cliquer dessus pour avoir accès à un rapport détaillé sur le degré de confidentialité qui lui est assuré.

Démonstration d'un produit TPVP destiné aux entreprises

M. Norman McConkey, Directeur de Watchfire Ltd, a présenté dans les grandes lignes le fonctionnement de WebCPO, un outil d'audit du respect de la vie privée destiné aux entreprises, qui a été mis au point par Watchfire Ltd.

M. McConkey a situé cet outil dans son contexte, en expliquant que l'envergure mondiale du marché de l'information et du commerce sur l'Internet ainsi que les caractéristiques mêmes de l'Internet avaient accéléré l'évolution vers un accroissement de la collecte, de l'utilisation et du partage de l'information, et que les organisations devaient par conséquent maintenant évaluer comment les lois qui régissaient les activités commerciales ainsi que les questions découlant des atteintes à la vie privée dans le monde peuvent les affecter. Il a également fait remarquer que les problèmes concernant la protection de la vie privée sur le Web étaient à l'origine d'un mouvement général sur le marché qui occasionnait aux entreprises des manques à gagner et des pertes de débouchés ou nuisait à des marques et à des réputations. Tous ces facteurs conjugués soulignent l'importance primordiale que la gestion de la vie privée sur les sites Web revêt pour les entreprises, qui doivent agir pour conserver la confiance de leurs clients s'ils veulent tirer le meilleur parti des possibilités offertes par l'Internet et entretenir des relations profitables avec les utilisateurs.

M. McConkey a ensuite abordé la question des risques d'atteinte à la vie privée sur le Web pour les entreprises. Il a fait remarquer que les sites Web captaient une quantité considérable d'informations personnelles sensibles ou superflues et que les atteintes à la vie privée pouvaient découler d'une politique inadaptée ou non appliquée ; de l'absence de mesures de protection adéquates de la sécurité au point de collecte d'informations personnelles sensibles ; de l'utilisation de témoins de connexion et de pixels espions (« invisibles ») pour pister l'internaute ; ou de liens vers des tiers et de contenus intégrés de tiers.

Selon M. McConkey, pour éviter ce genre de situation, il importe que les entreprises commencent par créer et appliquer un programme de gestion des risques d'atteinte à la vie privée. M. McConkey a ensuite donné la démonstration du logiciel de gestion de la confidentialité pour les sites Web qui surveille et analyse automatiquement toutes les caractéristiques Web (Internet, intranet et extranet) de sorte que les organisations peuvent comprendre leurs pratiques en matière de collecte, d'utilisation et, le cas échéant, de

partage d'informations et éviter des dérapages. Conçu pour de grands environnements multi-utilisateurs, ce logiciel analyse un site Web et stocke les résultats de cette analyse dans une base de données centrale que les utilisateurs peuvent interroger pour obtenir automatiquement des rapports complets qui recensent les points susceptibles de poser des problèmes de confidentialité. En outre, les responsables de la protection de la vie privée et ceux qui assurent le contrôle de l'application des politiques en la matière sont automatiquement prévenus lorsque des modifications sont apportées dans des zones à haut risque du site Web (par exemple la modification non autorisée d'une déclaration de politique de protection de la vie privée). M. McConkey a fait la démonstration de ce logiciel en direct en l'utilisant pour analyser un site Web « victime d'effraction » créé pour les besoins de la démonstration et a montré comment les divers rapports pouvaient être produits.

M. McConkey a conclu sa présentation en faisant remarquer que la plupart des règles en matière de confidentialité n'étaient pas transgressées intentionnellement mais que les entreprises devaient accorder davantage d'importance à la conformité avec ces règles et au contrôle de conformité si elles voulaient que le commerce électronique inspire confiance aux consommateurs.

Prise en main des produits technologiques présentés

Les participants ont ensuite été invités à naviguer sur l'Internet en utilisant les technologies destinées aux particuliers sur des ordinateurs mis à leur disposition par l'OCDE. Des agents de l'OCDE et les conférenciers pouvaient prêter assistance aux participants et leur donner des compléments d'explication sur les fonctionnalités des technologies.

Débat général, questions-réponses

Le débat général a mis en évidence les points ci-après :

- Il a été demandé à M. McConkey si Watchfire Ltd. utilisait une norme pour effectuer un audit des pratiques de protection de la vie privée qui ont cours sur un site Web et si les lignes directrices de l'OCDE servaient de base à cet audit. M. McConkey a fait remarquer que les problèmes de protection des données, lorsqu'ils se posent dans quelque juridiction que ce soit, entrent en général dans quatre catégories, à savoir collecte des données, partage des données, diffusion accidentelle des données et maintien de la cohérence entre l'intention d'une entreprise (c'est-à-dire sa déclaration de politique de protection de la vie privée) et son action (c'est-à-dire ce qu'elle fait dans la pratique à cet égard). Il a expliqué que le programme WebCPO consistait à analyser le site Web d'entreprise en vue d'y déceler d'éventuels problèmes, de façon que le personnel soit en mesure d'apporter les améliorations nécessaires pour assurer la conformité aux lois/principes/lignes directrices applicables.
- Le protocole P3P a suscité un débat et des éclaircissements détaillés ainsi qu'une certaine confusion parmi les participants, qui se demandaient s'il s'agissait d'une procédure plus poussée que la gestion des témoins. Mme Lindskog a confirmé que le filtrage des témoins de connexion constituait l'un des aspects du protocole P3P mais que celui-ci allait bien au-delà. Il s'agit d'un outil destiné à aider l'internaute à avoir facilement accès à la politique de protection de la vie privée d'un site Web et à lui permettre de la comparer aisément avec ses propres critères en la matière. Mme Valet-Harper a indiqué qu'Internet Explorer 6 de Microsoft permet à l'internaute d'utiliser cette technologie pour déterminer s'il veut fournir de l'information ou bloquer des témoins qui communiquent une information nominative.

- Le problème lié au fait qu'il n'est pas possible de concrétiser véritablement les pratiques protectrices qui sont présentées par les TPVP a été soulevé. Ces technologies peuvent en effet offrir certaines protections mais il n'existe souvent pas de moyens de vérifier si le degré de protection effectivement assuré correspond à ce que les TPVP sont censés fournir.
- Il a été mentionné que la technologie P3P pouvait être anticoncurrentielle. Si un site Web ou une entreprise applique une bonne politique de confidentialité mais ne met pas en œuvre le protocole P3P, est-ce que son trafic ne sera pas détourné ?
- Enfin, la question a été soulevée de savoir s'il serait indiqué de travailler à l'élaboration de normes internationales de gestion (cette question est actuellement examinée dans le cadre européen).

Session II: Éduquer les utilisateurs/consommateurs et les entreprises

Cette session mettait plus particulièrement l'accent, à travers une série de présentations, sur les questions à prendre en considération et les méthodes à utiliser pour éduquer les internautes/consommateurs et les entreprises à l'usage des TPVP. Un spécialiste a donné un aperçu de la nature de la perception des risques d'atteinte à la vie privée chez les particuliers et de la place qui revient dans ce contexte à une campagne de sensibilisation aux TPVP. Ont ensuite pris la parole, dans une optique plus pragmatique, deux conférenciers qui ont abordé respectivement le concept de « protection de la vie privée à la source » et la sensibilisation des internautes/consommateurs.

Perception des risques d'atteinte à la vie privée et sensibilisation aux TPVP

M. Perri 6, directeur du *Policy Programme* de l'*Institute for Applied Health and Social Policy*, du *Kings College* de Londres, a présenté l'étude qu'il avait réalisée en qualité de consultant auprès de l'OCDE (voir appendice II). M. 6 a expliqué qu'il s'attacherait surtout aux interrelations entre la perception des risques d'atteinte à la vie privée et la sensibilisation aux TPVP.

L'un des principaux points de l'intervention de M. 6 a été que, s'agissant de concevoir des mesures de sensibilisation efficaces des entreprises et des consommateurs, la question de la sensibilisation et de l'éducation devait être examinée sous l'angle de la *persuasion.* Selon lui, en effet, la question de savoir si les entreprises peuvent être persuadées ou non d'investir dans les TPVP – et si les consommateurs peuvent être persuadés de demander ces technologies – est un facteur décisif pour déterminer quand, pour qui et dans quelles conditions la « communication » au sujet des TPVP sera la plus efficace.

S'agissant des entreprises, M. 6 a souligné que la difficulté consistait à les persuader qu'elles devraient internaliser certains coûts (pour investir dans les TPVP) dans un marché où elles craignent que leurs concurrents n'externalisent ces coûts. En ce qui concerne les consommateurs, il a fait observer que la difficulté de la persuasion était déterminée, d'abord, par le degré d'importance que différents types de consommateurs attachent aux risques d'atteinte à la vie privée et par les risques qui les préoccupent le plus ; ensuite, par les modalités selon lesquelles se fait l'arbitrage entre les préférences en matière de protection contre divers types de risques et les augmentations de prix ; et enfin, par la façon dont les consommateurs font leur arbitrage entre leurs préférences en matière de confidentialité et le coût attaché à la recherche et au changement de fournisseurs.

Par ailleurs, selon M. 6, il faut déterminer « qui peut être persuadé de quoi », compte tenu des perceptions différentes et particulières du risque. A son avis, tout le monde ne montrera pas la même sensibilité à la persuasion pour tout, mais une classification et une segmentation des entreprises et des consommateurs permettent de comprendre plus facilement les différents degrés d'ouverture à la persuasion

– ou de « persuasibilité », étant donné que c'est la situation et le contexte institutionnel qui détermineront l'information que quelqu'un peut entendre, accepter ou rejeter.

Dans son analyse de la persuasibilité, M. 6 a d'abord segmenté les populations d'entreprises et de consommateurs selon des critères pertinents en insistant sur le fait que c'est en regroupant les entreprises par segments et en regroupant les consommateurs selon leur situation dans l'organisation sociale que l'on peut expliquer la perception des risques. Il a ainsi distingué les catégories d'activités suivantes : secteur « contrevenant », secteur bien régulé, secteur entreprenant et secteur « sous les projecteurs », et a regroupé les consommateurs dans les catégories isolément, hiérarchie, individualisme et enclave. Il a ensuite déterminé les types de protection de la vie privée qui pourraient susciter le plus grand intérêt dans chaque segment/groupe et a parlé des moyens qui seraient les plus efficaces pour persuader chacun de ces segments/groupes.

M. 6 a ensuite abordé la question de la dynamique de la relation entre d'une part la capacité et la volonté des entreprises d'offrir des services respectant la vie privée, et d'autre part la capacité et la volonté des consommateurs de demander ces services. Il a noté qu'il était possible, dans le cadre des processus institutionnels régissant les entreprises et les consommateurs, qu'il se crée un processus de tri amenant à graviter les uns vers les autres les consommateurs et les entreprises présentant des similitudes dans leurs caractéristiques, les cadres institutionnels dans lesquels ils évoluent, les contraintes auxquelles ils sont soumis et leurs préoccupations. Il a souligné que ce processus de tri n'était jamais parfait étant donné la dynamique du marché, et a fait remarquer qu'il serait possible de parvenir à un degré raisonnable de tri entre les différents segments d'entreprises et de consommateurs.

Dans sa conclusion, M. 6 a formulé les observations suivantes à l'intention des responsables politiques qui s'efforcent de convaincre les entreprises et les consommateurs de l'utilité des TPVP. Il existe des possibilités de persuader les entreprises et les consommateurs de s'intéresser aux TPVP, mais elles sont limitées par le fait que certains types de TPVP seront plus attrayantes pour les entreprises et les consommateurs dans certaines situations. En gardant présent à l'esprit la diversité des contraintes, des contextes institutionnels, des hypothèses fondamentales et des perspectives des entreprises et des consommateurs, le responsables de l'action gouvernementale seront capables de cibler leurs efforts de communication concernant les TPVP sur des groupes précis d'entreprises et de consommateurs, et produiront ainsi un effet déterminant.

Protection de la vie privée à la source

Mme Stéphanie Perrin, Responsable de la protection de la vie privée chez Zero-Knowledge Systems Inc., a fait le point sur les progrès réalisés en matière de protection de la vie privée à la source.

Mme Perrin a d'abord donné un aperçu de l'expérience de Zero-Knowledge, depuis la création de cette entreprise, en 1997, et en a décrit les principaux produits. Elle a expliqué que Zero-Knowledge s'attachait essentiellement à développer des outils pour les consommateurs et que son produit phare était *Freedom Premium Services 2.2* qui permet aux consommateurs de reprendre le contrôle total de leur vie privée, de créer leur propre identité, de décider ce qu'ils veulent révéler et à qui et de se protéger contre le pistage et l'établissement de profils. Cependant, constatant que la demande des consommateurs s'orientait vers des outils de protection de la vie privée et de sécurité, Zero-Knowledge a récemment remanié et remplacé *Freedom Premium Services 2.2* par *Freedom Privacy and Security Tools 3.0*. Ce nouveau produit est un progiciel de sécurité et de protection de la vie privée en ligne qui consiste en un pare-feu personnel appuyé par une suite flexible d'applications (comprenant un logiciel de formulaires/gestionnaire de mots de passe, un gestionnaire de témoins de connexion, un gestionnaire de publicité et une alerte par mots-clés)

permettant au consommateur de sécuriser son PC contre toute menace informatique tout en protégeant sa vie privée et l'information personnelle qui le concerne sur l'Internet.

L'autre produit phare de Zero-Knowledge est l'*Enterprise Privacy Manager* (EPM), un outil qui a pour but d'aider les organisations à exercer une gestion sécurisée et privée des données de leurs clients et des leurs. Ce produit permet aux entreprises d'identifier, d'analyser, de gérer et de notifier l'emplacement et le traitement de l'information du client dans toute l'entreprise. Zero-Knowledge l'a mis au point parce que les organisations collectent et stockent un volume croissant d'information mais éprouvent des difficultés à la gérer efficacement. Le produit est un outil automatisé qui aide à résoudre ce problème en permettant aux entreprises de réduire leurs coûts de fonctionnement et de conformité à la réglementation, de fidéliser leurs clients et de renforcer leur confiance, et d'atténuer les risques liés à la gestion de l'information.

Mme Perrin a expliqué que Zero-Knowledge fournissait en outre des services de conseils techniques, de formation et de développement pour aider les compagnies dans un certain nombre de domaines, que ce soit pour établir les priorités du plan de protection de la vie privée d'une entreprise, analyser les pratiques en matière de traitement de l'information ou adapter le système EPM à l'environnement particulier d'une entreprise pour en assurer l'intégration harmonieuse.

Enfin, Mme Perrin a évoqué certaines des difficultés que pose la communication d'informations relatives à la protection de la vie privée à la source aux consommateurs comme aux entreprises. Elle a recensé un certain nombre de problèmes de fond : les TPVP sont encore très mal comprises ; les consommateurs éprouvent des réticences à payer pour que leur vie privée et leur sécurité soient protégées et souffrent de « surcharge informationnelle » sur les nouvelles questions ; il faut rappeler aux entreprises l'importance qu'il y a à mettre en place des mécanismes de gestion des risques d'atteinte à la vie privée/sécurité, et leur fournir des incitations à investir ; les questions de l'application des lois et de la rétention des données demeurent problématiques et ont provoqué un refroidissement du marché ; les questions concernant l'authentification ne sont toujours pas résolues ; et les applications les plus récentes (par exemple, l'Internet sans fil et la géolocalisation) sont telles que le problème posé par l'intégration d'une protection de la vie privée « à la source » est loin d'être simple et pourrait bien être insoluble.

Sensibilisation des consommateurs aux TPVP

Mme Naja Felter, Chargée de mission, Commerce et cybercommerce, *Consumers International* (CI), a abordé les questions concernant la sensibilisation des consommateurs aux TPVP. Mme Felter a commencé son exposé en présentant des informations générales sur CI et en donnant une vue d'ensemble des initiatives de cet organisme en matière d'éducation. CI contribue à la sensibilisation du public essentiellement en publiant divers rapports, en formant des groupes membres nationaux et en entretenant des relations avec les milieux d'affaires internationaux. S'agissant d'éduquer efficacement les consommateurs, particulièrement en ce qui concerne les TPVP, Mme Felter a fait remarquer que la barre devait être placée bas car les gens qui ont le plus besoin d'aide en matière de protection de la vie privée sont probablement ceux qui ont des connaissances techniques assez élémentaires.

Mme Felter a récapitulé les résultats de la publication Privacy@Net de CI, qui rend compte d'une enquête internationale sur la protection privée dans le cybercommerce. Cette enquête a porté sur les pratiques des sites Web en matière de collecte de données. Sur les 751 sites examinés, deux tiers collectaient divers types de renseignements à caractère personnel, mais rares étaient ceux qui appliquaient des politiques de protection de la vie privée fournissant des renseignements sur les droits des internautes à l'égard des données. En outre, l'enquête de CI a révélé que parmi les sites qui s'étaient donné une politique de protection de la vie privée, plusieurs la transgressaient.

Selon Mme Felter, la protection de la vie privée et la sécurité, l'accès à des recours et la prévention de la fraude revêtent une importance primordiale pour les consommateurs, mais les TPVP ne peuvent qu'aider jusqu'à un certain point les consommateurs cherchant à protéger leur vie privée. Les principales faiblesses de ces technologies sont qu'elles ne sont pas faciles à utiliser et que les consommateurs ne sont par conséquent pas en mesure de prendre des décisions informées, et qu'elles ne couvrent qu'un sous-ensemble des pratiques loyales en matière d'information définies dans les Lignes directrices sur la protection de la vie privée. De plus, Mme Felter a noté que les TPVP étaient souvent présentées comme pouvant se substituer aux protections juridiques plutôt que comme un complément de celles-ci et que cela était regrettable car les TPVP ne sont, au mieux, qu'une solution imparfaite.

Mme Felter a conclu son intervention en faisant remarquer que CI encourage la mise au point de nouvelles TPVP comme complément du cadre juridique qui réglemente la collecte des données mais est d'avis que ce n'est pas aux consommateurs d'en supporter la charge. Mme Felter a aussi fait remarquer que les entreprises devraient par conséquent être incitées à intensifier leurs efforts pour que les TPVP mettent plus rigoureusement en œuvre et appliquent véritablement les Lignes directrices de l'OCDE en matière de protection de la vie privée et qu'elles puissent être beaucoup plus facilement utilisées de façon à offrir une utilité et une efficacité accrues pour la protection de la vie privée.

Débat général

Au cours du débat, les participants ont posé un certain nombre de questions précises se rapportant aux exposés :

- Il a été demandé à M. Perri 6 d'indiquer le pourcentage de consommateurs entrant dans chacune des catégories ou groupes définis dans son étude. M. 6 a indiqué que les consommateurs passaient d'un groupe à l'autre selon le contexte. Par exemple, ils peuvent être plus « enclavés » en ce qui concerne les données relatives à leur santé que pour les données relatives à leur identité qui sont stockées sur une carte de fidélité de supermarché. M. 6 a souligné que pour comprendre ce qui détermine la perception des risques, un complément d'étude est nécessaire pour examiner comment les individus d'une collectivité se comportent lorsque le contexte change. Il a également insisté sur la nécessité de disposer de données empiriques/économiques plus complètes dans le domaine de la protection de la vie privée car on ne dispose actuellement pas de données quantitatives de bonne qualité sur une base internationale. M. 6 a enfin souligné combien il importait d'adapter les stratégies de sensibilisation et de persuasion à la situation particulière du public visé.
- Il a été demandé à Mme Stéphanie Perrin de développer le concept de « marquage de données » correspondant à des droits/obligations en matière de protection de la vie privée et d'expliquer comment ce concept était mis en pratique. Mme Perrin a indiqué qu'il s'agissait de tenter de marquer les données dans un premier temps en tenant compte du fait que la plupart des grandes organisations ne sont pas toujours sûres de la provenance des données qu'elles reçoivent et des droits qui y sont attachés ou des promesses faites lorsqu'elles sont reçues. L'idée est par conséquent de coder tous les droits à l'information et bloquer l'information dès réception de sorte que les juristes puissent alors prendre une décision sur ce qu'il en adviendra.
- Il a été demandé à M. David Banisar, en sa qualité de représentant de *Consumers International*, de fournir des exemples pratiques d'action de sensibilisation. M. Banisar a expliqué que les nombreuses associations de consommateurs qui font partie de *Consumers International* mènent des activités diverses. Elles publient des rapports à l'intention des consommateurs et des études sur la protection de la vie privée, elles mènent des campagnes d'information dans les médias, et engagent des poursuites en justice et des actions de boycottage. CI espère également que certains

groupes importants procéderont à des tests d'utilisabilité et de vérification. L'organisme a également publié son document intitulé *Five Ways to Improve Privacy Online*, en cinq langues. Les recommandations du Conseil de l'Europe et de l'*Electronic Frontier Foundation* sur la façon dont les consommateurs peuvent se protéger sur l'Internet ont également été notées.

- Mme Stéphanie Perrin a ajouté des observations concernant les stratégies de sensibilisation des entreprises. Celles mises en œuvre par Zero-Knowledge s'appuient sur de l'information générale qu'elle diffuse sur son site Web (expliquant, par exemple, pourquoi les entreprises ont besoin de ces outils), la publication d'une lettre d'information, les réponses à des questions ponctuelles sur des sujets liés à la protection de la vie privée et la tenue de conférences annuelles sur la protection de la vie privée à la source en vue d'encourager les entreprises à intégrer la vie privée à la conception de leurs produits, de façon à fidéliser la clientèle et à renforcer sa confiance. Mme Perrin a fait remarquer que l'éducation des consommateurs était importante mais que les entreprises devaient également être encouragées à mener une réflexion sérieuse sur ces questions.
- S'agissant des questions de protection de la vie privée dans l'environnement des communications mobiles, qui ressort comme un thème générateur d'une nouvelle problématique à l'avenir, Mme Lindskog a souligné que l'évolution de l'industrie du sans fil indiquait que l'identité des utilisateurs se trouverait dans un appareil et que les problèmes de protection de la vie privée dans ce contexte devront par conséquent être réévalués.

Remarques de conclusion

Le président a annoncé la clôture du Forum en remerciant les conférenciers et les participants pour leur contribution. Il a noté la diversité des questions qui avaient été abordées ainsi que la nécessité que les pouvoirs publics, les entreprises, les spécialistes de la protection de la vie privée et les porte-parole des consommateurs poursuivent leurs efforts afin de sensibiliser les utilisateurs et les entreprises aux TPVP, de renforcer la confiance des utilisateurs dans ces outils et d'influencer leur développement dans l'intérêt d'une protection accrue de la vie privée.

NOTES

1. www.ntia.doc.gov/ntiahome/privacy/

2. Voir Chapitre 12.

3. Ibid.

4. M. Burkert est attaché à l'*Institute for Media Communication* du Centre national de recherche allemand sur les technologies de l'information – GMD.

5. Une enquête réalisée en mars 2000 par *Business Week/Harris* a par exemple révélé que 63 % des internautes qui n'avaient jamais rien acheté en ligne craignaient fort que l'entreprise auprès de laquelle ils pourraient acheter des produits n'utilise l'information à caractère personnel les concernant pour leur adresser de l'information non désirée. Un sondage Gallup effectué en septembre 2000 a révélé que 53 % des internautes étaient très préoccupés par la confidentialité des renseignements personnels qu'ils divulguaient en ligne et de leurs activités dans le cyberespace. L'hebdomadaire *The Economist* observait en octobre 2000 que le plus important obstacle au succès du commerce électronique était la peur qu'éprouvaient les clients à l'idée que des renseignements d'ordre financier les concernant soient mis en circulation dans le cyberespace.

6. Voir par exemple les conclusions des groupes spécialisés dans le cadre du rapport intitulé « Consumer Privacy in the Information Age », publié par le *National Consumer Council* du Royaume-Uni en décembre 1999.

7. Voir p. 33 et, en général, « Appendix 3 : Technologies of Privacy ».

8. D'autres organismes des pays membres ont publié des déclarations en faveur de la norme P3P et d'autres technologies protectrices de la vie privée.

9. « A Survey of Consumer Privacy Attitude and Behaviors », enquête menée pour la *Privacy Leadership Initiative* par Harris Interactive, rendue publique le 2 avril 2001. Alors que l'enquête révèle une faible utilisation des technologies protectrices de la vie privée, elle montre que les usagers sont sensiblement plus nombreux à prendre d'autres mesures pour protéger leur vie privée, en lisant notamment des politiques de protection de la vie privée, en refusant de communiquer de l'information qu'ils estiment trop personnelle ou superflue, et en évitant de visiter certains sites Web dont les pratiques en matière de respect de la vie privée sont douteuses.

APPENDICE I. ÉTUDE DES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE[1]

Objectif, périmètre et méthode

Objectif

L'objectif de cette étude est d'identifier les technologies visant à protéger la vie privée sur Internet et d'en préciser l'impact sur la protection de la vie privée au regard des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontière de données à caractère personnel.

Périmètre de l'étude

Cette recherche a privilégié les outils spécifiques au Web et, dans une moindre mesure, ceux relatifs à la messagerie. Elle n'a aucune vocation exhaustive. La priorité a été de se concentrer sur les outils ayant les fonctionnalités suivantes :

Fonctionnalité	Définition
Chiffrement	Utilisation importante mais non exclusive de la cryptographie
Anonymat/ pseudonymat	Rend l'utilisateur anonyme ou masque son identité grâce à un pseudonyme
Gestion de données personnelles	Management des préférences. Tout moyen qui permet de décider des informations susceptibles d'être collectées
Filtrage de cookies	Filtrage ou gestion des cookies
Filtrage de la publicité	Filtrage ou blocage des publicités
Filtrage de logiciels « spyware »	Détection et suppression des spywares. Spyware étant entendu comme : *i)* des gifs invisibles ou *ii)* des logiciels de publicité visant une clientèle spécifique [*client side ad software*]
Gestion du marketing avec consentement	Solution de marketing direct dans le respect de la vie privée
Protection des méls	Protection des méls par la sécurisation et/ou l'anonymisation
Sécurité des paiements en ligne	Sécurité des paiements en ligne
Contrôle de l'accès	Gestion centralisée des mots de passe
Audit d'audit et de conformité	Audit des moyens mis en place et de la conformité de ces moyens avec les principes de protection en vigueur
Didacticiel	Application éducative
Schéma complexe	Schéma technique complexe permettant de protéger la vie privée (par exemple : encirq)

1. Cette étude a été réalisée par Laurent Bernat, Directeur, Information et stratégie, Projetweb en tant que consultant auprès de l'OCDE.

On examine également les effets au regard des lignes directrices sur la protection de la vie privée :

- Sécurité.
- Limitation de la collecte/ choix.
- Empêchement de la collecte.
- Notification.
- Limitation de l'usage.
- Accès.
- Didacticiels/ information/ « éducation »
- Responsabilité.

Compte tenu des contraintes de temps et de ressources, n'ont pas pu être traités les outils présentant les fonctionnalités principales suivantes :

- Outils de cryptographie purs (par exemple : PGP).
- Outils orientés vers la protection des enfants (par exemple : MS Kids passport).
- Outils d'effacement des données (*deletion tools*), qu'il s'agisse de suppression définitive des traces physiquement laissées sur le disque en général (*true deletion*) ou de l'effacement normal des traces laissées en naviguant sur Internet (cookies, fichiers caches temporaires, historique, etc.).
- Outils destinés à assurer la sécurité réseau du PC : firewalls personnels et professionnels, anti-virus, analyseurs de trafic réseau (*packet sniffers*).
- Outils de sécurisation d'accès préservant l'anonymat, par exemple via un dispositif biométrique (par exemple : mytec.com)

Les solutions type « bouquet de services » proposées par les fournisseurs d'accès Internet (FAI) et les hébergeurs n'ont également pas pu être pris en compte.

Méthode

La recherche de ces outils a été effectuée à partir :

- Des répertoires généraux grand public (yahoo.com, about.com).
- Des moteurs de recherche (google.com, alltheweb.com).
- De bases de données de logiciels à télécharger (download.cnet.com).
- De sites de référence dans le domaine de la protection de la vie privée (epic.org, cdt.org, etc.).

Plus de 130 sites ont été visités, dont 83 ont été retenus comme proposant un outil permettant d'améliorer la protection de la vie privée selon le périmètre retenu (voir ci-dessus).

Ont été supprimés de la liste finale les sites :

- Manifestement obsolètes.
- Dont la crédibilité a été jugée médiocre d'après leur contenu (par exemple : un anonymiseur qui vante sur la moitié de sa page d'accueil les vertus aphrodisiaques des phéromones[2]).
- Dont les produits ne sont pas encore disponibles, même en version beta.
- Qui étaient indisponibles ou inaccessibles au moment du test (ces sites ont été visités plusieurs fois).

Il convient de noter que la présence d'un site en état de fonctionnement ne garantit pas que l'entreprise qui en est responsable soit encore en activité.

Chaque outil a été analysé au travers :

- De la présentation du produit disponible sur le site.
- D'un test succinct, le cas échéant.

De cette analyse découle une ventilation (voir la grille ci-jointe) qui distingue :

- Les informations sur l'entreprise : organisation et URL, type d'organisation, date de fondation, origine géographique, présence d'une politique de protection de la vie privée sur le site.
- Le nom du produit et, le cas échéant, sa version.
- Les informations sur le produit : caractéristiques, fonctionnalités principales, effet juridique au regard des lignes directrices de l'OCDE, cibles principales.

Chiffres

Les données ci-dessous récapitulent les chiffres :

Nombre de sites visités et retenus	83	
Audience ciblée		
Personnes physiques	69	83%
Personnes morales	17	20%
Origine géographique		
États-Unis	63	76%
Canada	6	7%
International (par exemple : W3, OCDE)	3	4%
?	2	2%
Allemagne	2	2%
Russie	2	2%
France	1	1%
Gibraltar	1	1%
Suède	1	1%
Thaïlande	1	1%
Royaume-Uni	1	1%

2. www.aixs.net.

La recherche ayant été faite à partir de mots-clés saisis en anglais, il est possible que des outils n'aient pas été identifiés si les sites qui les présentent étaient rédigés dans une autre langue. Ceci peut relativiser la faible présence d'outils présentés sur d'autres sites que des sites nord-américains.

Présence d'une politique de protection de la vie privée sur le site		
Oui	63	75%
Non	20	25%
Type d'application		
Basée sur le Web	24	29%
A installer.	42	51%
Basée sur le Web/ à installer.	4	5%
A installer (java).	2	2%
A installer (ActiveX).	1	1%
Autres	10	12%
Contre paiement ou gratuit		
Contre paiement	30	36%
Gratuit	38	46%
Tous les deux	11	13%
Pas clair	4	5%
Inscription obligatoire	9	11%
Abonnement obligatoire	14	17%
Fonctionnalité principale		
Chiffrement	16	19%
Anonymat/ pseudonymat	30	36%
Gestion des données personnelles	10	12%
Filtrage de cookies	39	47%
Filtrage de la publicité	15	18%
Filtrage de logiciels spyware	15	18%
Gestion du marketing avec consentement	2	2%
Protection des méls	15	18%
Sécurisation des paiements	4	5%
Contrôle de l'accès	5	6%
Audit de protection et de conformité	6	7%
Didacticiel	2	2%
Schéma complexe	7	8%
Effet politique		
Sécurité	22	27%
Limitation de la collecte des données	37	45%
Empêchement de la collecte de données	33	40%
Notification	11	13%
Limitation de l'usage	2	2%
Accès	2	2%
Didacticiels/ information/ « éducation »	2	2%
Transparence/responsabilité	4	5%

Synthèse

L'examen des caractéristiques des outils et le repérage de leurs limites confirment à la fois l'intérêt de leur utilisation par les internautes pour protéger la vie privée et leur caractère nécessairement complémentaire par rapport à d'autres outils, qu'ils soient éducatifs, contractuels, réglementaires ou autres.

Bénéfices et limites

Sur un plan technique, aucun des outils identifiés n'exploite un panel de fonctionnalités complet permettant de protéger totalement la vie privée des personnes au regard des principes des lignes directrices de l'OCDE.

Si l'on comptabilise le nombre d'outils ayant un impact sur les principes des lignes directrices de l'OCDE, on constate que :

- Un seul outil concerne cinq des huit principes[3].
- Deux outils en concernent trois[4].
- Quarante-quatre outils en concernent deux.
- Cinquante-huit en concernent un seul.

Aucun outil identifié dans cette étude ne propose donc une solution complète de protection de la vie privée. Un utilisateur qui souhaiterait se protéger le plus efficacement possible devrait donc combiner plusieurs outils pour optimiser son niveau de protection.

Marketing avec consentement et vie privée : naissance d'un nouveau marché ?

Les outils et solutions découverts dans cette étude constituent un marché émergent : à la demande des utilisateurs en matière de protection de leur vie privée sur Internet répond une offre divisée en plusieurs segments. Certaines entreprises proposent des solutions originales d'intermédiation technologique (proches du concept d' « infomédiaire » développé par John Hagel et Marc Singer[5]) dont l'objectif est de permettre aux entreprises d'exploiter des données personnelles à des fins de marketing avec le consentement de l'utilisateur (*permission based marketing*) et en garantissant le respect de sa vie privée. Elles semblent très récentes et être à l'heure actuelle en recherche de partenariats économiques et financiers[6].

3. Outil d'audit/conformité destiné aux entreprises (TrustFilter de PrivacyRights).

4. Freedom Internet Privacy Suite de Zero Knowledge, destiné aux internautes et Tivoli Secure Way Manager d'IBM, destiné aux organisations.

5. « Net Worth », Harvard Business School, 1999.

6. On notera, à titre d'exemple, les solutions de Lumeria, Encirq et Persona.

Freins techniques à la généralisation

Parmi les outils examinés dans cette étude, 51 % requièrent une installation sur l'ordinateur de l'internaute. Cette installation peut parfois constituer un frein à leur généralisation :

- Perçue comme potentiellement dangereuse par l'utilisateur, l'installation peut être refusée par ce dernier.
- Contraire à la politique de l'entreprise qui, souvent, interdit l'installation d'applications non standardisées sur les postes des collaborateurs, elle peut placer le salarié dans une situation ambiguë à l'égard de son employeur et lui faire prendre des risques en contradiction avec sa volonté de protéger sa vie privée.

Par ailleurs, pour qu'un produit soit largement répandu, il doit être compatible avec l'ensemble des systèmes d'exploitation disponibles et, lorsqu'il fonctionne en tant que « *plug-in* » du navigateur, il doit être disponible pour plusieurs versions de ce dernier. En réalité, cette universalité est rarement atteinte par ces produits, leurs éditeurs concentrant la compatibilité sur une ou deux versions des systèmes d'exploitation ou navigateurs du marché.

Freins psychologiques : le poids de la confiance

Certains sites présentent très peu d'informations sur l'organisation qui en est responsable, son pays d'origine, sa nature (société commerciale, association, personne physique) et l'identité des fondateurs ou même ses coordonnées exactes. Souvent, seule une adresse mél relie l'utilisateur à l'éditeur du site.

Certains sites gratuits sont parfois dénués de toute information permettant de situer leur origine, y compris en interrogeant la base de données Whois pour identifier le possesseur du nom de domaine du site[7]. Quant aux produits payants, qui requièrent un paiement à distance pour disposer du produit, ils ne présentent pas toujours toutes les informations nécessaires.

Pour qu'un outil de type PET soit utilisé par les internautes, ces derniers doivent pouvoir accorder leur confiance :

- A la technologie utilisée par l'outil. L'utilisateur doit donc la comprendre et en saisir les enjeux.
- A l'outil lui-même : est-il stabilisé, sans failles ni bogues qui, au lieu de protéger l'utilisateur, pourraient accroître sa vulnérabilité ?
- A l'organisation ou la personne physique qui l'a développé : poursuit-elle réellement les buts qu'elle annonce ?

7. Par exemple : www.the-cloak.com, interface Web permettant d'anonymiser la navigation via un proxy. Aucune information sur l'origine du service ou ses responsables n'est disponible sur le site. Les informations de la base de données Whois, ne permettent pas d'identifier clairement son pays d'origine.

Les logiciels issus de la communauté Open Source présentent un niveau de transparence élevé. Plusieurs projets Open Source en cours de développement sont spécifiquement orientés vers la protection de la vie privée.

L'éducation des utilisateurs

Il ressort de ce qui précède que l'éducation des utilisateurs est une composante indispensable de l'ensemble des politiques visant la protection de la vie privée en ligne. A cet égard, de nombreux sites visités présentent une dimension pédagogique importante sans laquelle les produits qu'ils proposent ne pourraient pas convaincre leur public.

On distinguera trois attitudes différentes de la part des sites visités :

- Les sites présentant des technologies en cours de développement et donc plutôt destinés à des utilisateurs avancés, qu'ils soient utilisateurs de pointe « power users » ou développeurs[8]. L'information est alors très détaillée et très technique, vraisemblablement trop pour l'utilisateur final.
- Les sites associant leur documentation commerciale ou la présentation de leurs motivations à des informations à caractère pédagogique de bonne qualité[9] et des liens vers d'autres sites de référence.
- Les sites qui privilégient la description des avantages et bénéfices de l'outil sans véritablement informer les utilisateurs sur la relation entre le bénéfice en question (l'anonymat, par exemple) et le fonctionnement technique du produit.

Travaux ultérieurs possibles

Optimisation de la classification des fonctionnalités techniques

Une classification plus complète des fonctionnalités et des techniques utilisées, assortie de définitions pointues, permettrait de mieux qualifier le lien entre la technique et son effet juridique.

A titre d'exemple :

- Concernant les cookies, on pourrait distinguer l'affichage, le blocage, le filtrage, l'édition, la suppression et la distinction des cookies provenant de sites tiers. Certains outils peuvent limiter la collecte via un choix ou bien empêcher systématiquement la collecte selon les fonctionnalités présentes.
- Pour les outils d'anonymisation via proxy non transparent, on pourrait distinguer :
  - Ceux qui utilisent leur propre proxy.
  - Ceux qui sélectionnent, testent et exploitent d'autres proxies, augmentant ainsi considérablement le degré d'anonymat de l'utilisateur.

---

8. Par exemple, le site du projet Freenet (http://freenet.sourceforge.net) ou encore l'éditeur de politiques P3P d'IBM (www.alphaworks.ibm.com/tech/p3peditor).

9. Par exemple, le site de Anonymizer présente des informations claires sur le fonctionnement du produit et, par extension, sur le principe d'un anonymiseur par proxy (www.anonymizer.net).

- Ceux qui autorisent HTTPS pour brouiller les traces laissées sur le réseau local.
- Ceux qui filtrent certaines informations (cookies, dernière page visitée, publicités, javascript, images, etc.).

Un approfondissement de ces questions permettrait de prendre également en compte certaines subtilités techniques. Par exemple, un cookie persistant constitue un risque pour l'utilisateur à l'égard du site qui le place mais également à l'égard d'une tierce personne ayant accès à son disque dur. Ceci pourrait donc conférer aux outils de gestion des cookies un effet sur la « sécurité », au sens des lignes directrices de l'OCDE.

Étude spécifique de certains types d'outils

Les technologies laissées de côté pourraient faire l'objet d'une étude spécifique, par exemple :

- Les outils de cryptographie pure.
- Les outils relatifs à l'utilisation de la messagerie.
- Les outils de sécurisation personnelle.
- Les outils s'adressant plus spécifiquement aux enfants.
- Les outils exploitant d'autres protocoles que la messagerie ou le Web comme les groupes qui échangent des nouvelles (*newsgroups*), la discussion en direct (ICQ, IRC, AOL buddy list, etc.), telnet ou encore le transfert de fichiers (FTP) qui n'ont pas été abordés spécifiquement dans cette étude alors qu'ils se sont largement démocratisés.

Une attention toute particulière mériterait d'être apportée aux :

- Outils en cours de développement dans la communauté du logiciel libre : le mot-clé « *privacy* » dans le moteur de recherche du principal site qui regroupe ces projets[10] renvoie 25 projets en cours.
- Projets exploitant la technologie des réseaux distribués ou poste à poste (*peer-to-peer* ou encore P2P) et particulièrement, le projet Freenet dont l'objectif est précisément de garantir l'anonymat à ses utilisateurs, qu'ils publient de l'information ou la consultent.
- Outils ou technologies destinés à sécuriser un système ou l'accès à un système sans divulguer l'identité des utilisateurs (par exemple : mytec.com, cité plus haut).
- Outils ou solutions orientées vers le marketing avec permission qui respectent la vie privée de l'utilisateur.

Facilité d'utilisation des outils et vocation pédagogique

L'analyse de la facilité d'utilisation des outils pourrait apporter un éclairage intéressant. Il s'agirait essentiellement d'évaluer la capacité de l'utilisateur final à saisir pleinement le sens de chaque outil, à parvenir à l'installer efficacement et à l'utiliser en permanence et au quotidien.

Si peu d'outils ont une vocation principalement pédagogique visant l'éducation et la responsabilisation des utilisateurs, la plupart contribuent à une meilleure information de ces derniers et certains y attachent une assez grande importance. Il pourrait être intéressant d'identifier les outils qui

10. www.sourceforge.net.

présentent des fonctionnalités spécifiques pour atteindre cet objectif et d'analyser les moyens qu'ils mettent en place pour y parvenir.

Autres pistes

Une recherche plus approfondie des outils disponibles, c'est-à-dire visant l'exhaustivité, pourrait être effectuée, notamment en utilisant des termes de recherche dans des langues autres que l'anglais.

Tableau 1. **Technologies examinées**

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
@nonymouse http://nonymouse.com/	Association	1997 (droit d'auteur)	Oui	Allemagne	AnonWWW AnonEmail AnonNews	Gratuit. Disponible sur le Web.	Anonymat/ pseudonymat. Protection des méls.	Empêchement de la collecte.	Personnes physiques.
AbsoluteFuture, Inc. www.safemessage.com	Entreprise de logiciels	1998	Oui	États-Unis	SafeMessage v. 2.0	Payant. Abonnement obligatoire. A installer.	Chiffrement. Protection des méls.	Sécurité. Empêchement de la collecte.	Organisations.
adScience, Ltd.	Entreprise de logiciels	1997 ?	Oui	Royaume-Uni	Filtergate v. 4.03	Payant. A installer.	Filtrage de cookies. Filtrage de la publicité. Filtrage des spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Agenetics www.superyou.net	Entreprise sur Internet	?	Oui	États-Unis (nom de domaine)	SuperYou Messaging	Gratuit. Inscription obligatoire. Disponible sur le Web. Version beta.	Chiffrement. Protection des méls.	Sécurité.	Personnes physiques.
American Express www.americanexpress.com	Fournisseur de cartes de crédit	1850 (Private Payments : 2000)	Oui	États-Unis	Private Payments	Gratuit. Inscription obligatoire. A installer. Gratuit pour les détenteurs de cartes	Sécurité des paiements en ligne.	Sécurité. Limitation de la collecte/ choix.	Personnes physiques.
AnalogX www.analogx.com	Entreprise de logiciels?	1998 ?	Non	États-Unis	CookieWall v. 1.01	Gratuit. A installer. Se rajoute au navigateur.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Anonymizer www.anonymizer.com	Entreprise de protection de la vie privée et de sécurité	1996	Oui	États-Unis	Anonymous Surfing, Secure Tunneling	Payant. Abonnement obligatoire. Disponible sur le Web/ A installer. Version de base gratuite.	Anonymat/ pseudonymat. Filtrage de cookies. Filtrage de la publicité. Filtrage des spyware.	Empêchement de la collecte.	Personnes physiques.
AOL/Netscape www.netscape.com	FAI/ entreprise de logiciels	?	Oui	États-Unis	Netscape Cookie Manager, Password manager v. 6.1	Gratuit. Compris dans le navigateur	Filtrage de cookies. Contrôle de l'accès.	Sécurité. Limitation de la collecte/ choix.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Ascentive www.ascentive.com	Entreprise de logiciels	1998 (droit d'auteur)	Oui	États-Unis	ActivePrivacy v. ?	Payant. A installer. Gratuit pendant une période limitée.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
AT&T	Entreprise de télécommuni-cations \	AT&T établie en 1875	Oui	États-Unis	Crowds	Gratuit. Inscription obligatoire. A installer. Seulement pour un usage privé aux États-Unis.	Anonymat/ pseudonymat.	Empêchement de la collecte.	Personnes physiques.
AT&T www.research.att.com/projects/p3p/propgen	Entreprise de logiciels	AT&T établie en 1875	Oui	États-Unis	P3P proposal generator	Gratuit. Disponible sur le Web.	Gestion de données personnelles.	Notification.	Personnes physiques.
Barefoot Productions www.barefootinc.com	Entreprise de logiciels	1994 (société anonyme en 1997)	Non	États-Unis	Zdnet's CookieMaster v. 2.0	Gratuit. A installer. Produit périmé (seulement IE 3.0). Distribué par ZiffDavis, les liens à zdnet sont cassés.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Basta Computing www.basta.com	Entreprise de logiciels	1996	Oui	États-Unis	Buzof v. 1.6	Payant. A installer.	Filtrage de cookies. Filtrage de la publicité.	Limitation de la collecte/ choix.	Personnes physiques.
Camtech 2000, Ltd. www.camtech2000.net	Entreprise de logiciels ?	?	Non	États-Unis (nom de domaine)	CT Cookie Spy v. 2.0	Gratuit. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Checkflow www.flowprotector.com	Entreprise de logiciels	?	Oui	France	FlowProtector v. 2.0	Gratuit/ payant. A installer. Payant pour la version avancée.	Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Direct Marketing Association www.the-dma.org/privacy	Association professionnelle	1917	Oui	États-Unis	Générateur de politique de protection de la vie privée	Gratuit. Disponible sur le Web.	Gestion de données personnelles. Gestion de données personnelles.	Notification.	Organisations.
Disappearing Inc./ Omniva www.disappearing.com www.omniva.com	Entreprise de logiciels	1999	Oui	États-Unis	Omniva Policy Manager v. ?	Payant. A installer.	Chiffrement. Sécurité des paiements en ligne.	Sécurité.	Organisations.
Distinctly.com, Inc.	Entreprise de technologies Internet	1997 (nom de domaine)	Oui	États-Unis	SilentSurf	Gratuit. Disponible sur le Web.	Anonymat/ pseudonymat.	Empêchement de la collecte.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Ditto Technologies www.dittotech.com	Entreprise de logiciels	2000 (droit d'auteur sur le site)	Non	États-Unis	Cookie Eater	Gratuit. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Ditto Technologies www.dittotech.com	Entreprise de logiciels	2000 (droit d'auteur sur le site)	Non	États-Unis	MiLk v. 2.0	Payant. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Dr. Jon's Software www.angelfire.com/il2/drjsoftware/	Développeur individuel ?		Non	États-Unis	MagicCookie Monster v. 1.0 fc 1a	Gratuit. Inscription obligatoire. A installer. Inscription par mél.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Encirq www.encirq.com	Entreprise de protection/sécurité de la vie privée et de marketing	1998	Oui	États-Unis	Illuminated Statement	Payant. Outil commercial.	Anonymat/ pseudonymat. Schéma complexe.	Empêchement de la collecte.	Organisations.
Eric Murray Consulting www.meer.net/~ericm/cookie_jar/	Consultant en protection de la vie privée et sécurité	?	Non	États-Unis	Cookie Jar v. 2.01	Gratuit. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Free Network Project http://freenet.sourceforge.net/	Société à but non lucratif	1999	Non	États-Unis	Freenet v. 0.3.9.2	Gratuit. A installer. Version beta. Projet Open source. La société a été créé uniquement pour obtenir des dons.	Chiffrement. Anonymat/ pseudonymat. Schéma complexe.	Sécurité. Empêchement de la collecte.	Personnes physiques.
George Mason Society http://freedom.gmsociety.org	Groupe de pression	?	Non	États-Unis	Freedom remailer	Gratuit. Disponible sur le Web.	Anonymat/ pseudonymat. Protection des méls.	Empêchement de la collecte.	Personnes physiques.
Global Internet Liberty Campaign www.gilc.org/speech/anonymous	Groupe de pression	?	Non	International	W3-Anonymous Remailer	Gratuit. Disponible sur le Web.	Anonymat/ pseudonymat.	Empêchement de la collecte.	Personnes physiques.
Guidescope, Inc. www.guidescope.com/home	Entreprise de technologies Internet	2000	Oui	États-Unis	Guidescope v. 0.994	Gratuit/ payant. A installer. Gratuit pour usage personnel/ payant pour usage commercial	Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Hidden surf www.hiddensurf.com	Entreprise de protection de la vie privée sur Internet ?	?	Oui	États-Unis (nom de domaine)	Hiddensurf	Payant. Abonnement obligatoire. Disponible sur le Web.	Anonymat/ pseudonymat. Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Hilgraeve www.hypersend.com	Entreprise de logiciels de protection de la vie privée	1980	Oui	États-Unis	HyperSend	Payant. Inscription obligatoire. Abonnement obligatoire. Disponible sur le Web/ A installer.	Chiffrement. Protection des méls.	Sécurité. Empêchement de la collecte.	Personnes physiques.
Hush Communications www.hushmail.com	Entreprise de protection de la vie privée et de sécurité	1998	Oui	États-Unis	HushMail v. V2	Gratuit/ payant. Disponible sur le Web. Gratuit + redevance annuelle pour services de pointe	Chiffrement. Anonymat/ pseudonymat. Protection des méls.	Sécurité.	Personnes physiques.
IBM www.ibm.com	Entreprise de technologie informatique	1914	Oui	États-Unis	Tivoli SecureWay Privacy Manager	Payant. A installer. Outil commercial	Schéma complexe.	Sécurité. Use limitation. Access.	Organisations.
IBM www.ibm.com www.alphaworks.ibm.com/tech/p3peditor	Entreprise de technologie informatique	1914	Oui	États-Unis	P3P Policy Editor v. beta 1.7	Gratuit. A installer. Version beta.	Gestion de données personnelles.	Notification.	Personnes physiques.
Idcide www.idcide.com	Entreprise de protection de la vie privée et de sécurité	1999	Oui	États-Unis (Israël)	Privacy Companion v. 1.0.3	Gratuit. A installer. Se rajoute au navigateur.	Filtrage de cookies. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Idcide www.idcide.com	Entreprise de protection de la vie privée et de sécurité	1999	Oui	États-Unis (Israël)	PrivacyWall (Site Analyzer, Site Monitor)	Payant. A installer.	Audit / conformité.	Responsabilité.	Organisations.
IDzap, LLC www.idzap.com	Entreprise de protection de la vie privée et de sécurité	?	Oui	États-Unis	- Idsecure - navigation anonyme gratuit	Gratuit/ payant. Inscription obligatoire. Abonnement obligatoire. Disponible sur le Web. Abonnement pour service de pointe (idsecure). Gratuit pour service de base (navigation anonyme gratuite). Inscription par mél pour les deux.	Anonymat/ pseudonymat. Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Incogno Corporation www.incogno.com	Entreprise de logiciels	1999	Oui	États-Unis	SafeZone	Outil commercial.	Chiffrement. Anonymat/ pseudonymat. Sécurité des paiements en ligne. Schéma complexe.	Sécurité. Empêchement de la collecte.	Organisations.
INetPrivacy www.inetprivacy.com	Entreprise de logiciels de protection de la vie privée	1997 (droit d'auteur)	Non	Russie/ Canada (nom de domaine)	Anonymity Proxy (A4Proxy) v. 2.52	Payant. A installer.	Anonymat/ pseudonymat. Filtrage de cookies.	Limitation de la collecte/ choix. Empêchement de la collecte.	Personnes physiques.
Information and Privacy Commissioner/ Ontario www.ipc.on.ca/english/resources/resources.htm	Responsable de la protection de la vie privée	1990	Non	Canada (Ontario)	Privacy Diagnostic Tool (PDT)	Gratuit. A installer. Fichier MS Access.	Audit / conformité. Didacticiel	Didacticiels/ information/ connaissance.	Organisations.
Intelligent Software Modeling Inc. www.surferprotectionprogram.com	Entreprise de protection de la vie privée sur Internet	1997	Non	États-Unis	Surfer Protection Program	Payant. A installer.	Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.
Intelytics www.intelytics.com	Entreprise de logiciels de protection de la vie privée	?	Oui	États-Unis	Message sentinel	Payant. A installer.	Filtrage de spyware. Protection des méls.	Empêchement de la collecte.	Personnes physiques.
Intelytics www.intelytics.com	Entreprise de logiciels de protection de la vie privée	?	Oui	États-Unis	Personal Sentinel v. 1.5.2	Gratuit. Inscription obligatoire. A installer.	Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Intelytics www.intelytics.com	Entreprise de logiciels de protection de la vie privée	?	Oui	États-Unis	Site sentinel	Payant. A installer.	Audit / conformité.	Responsabilité.	Organisations.
Intermute www.intermute.com www.adsubtract.com	Entreprise de logiciels	?	Oui	États-Unis	AdSubtract	Gratuit/ payant. Inscription obligatoire. A installer. Gratuit pour usage personnel/ payant pour versions plus avancées.	Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Invisible hand software www.privacybot.com	Entreprise de logiciels	1991	Oui	États-Unis	PrivacyBot	Payant. Abonnement obligatoire. Disponible sur le Web.	Audit / conformité.	Notification. Responsabilité.	Organisations.
iPrivacy www.iprivacy.com	Entreprise de protection de la vie privée et de sécurité	1999	Oui	États-Unis	Identity Manager	Gratuit. Outil d'accès pour les consommateurs au travers les compagnies de cartes de crédit.	Chiffrement. Anonymat/ pseudonymat. Sécurité des paiements en ligne. Schéma complexe.	Sécurité. Empêchement de la collecte.	Personnes physiques.
ISL Internet Sicherheitsloesungen GmbH www.rewebber.de/index.php3.en	Entreprise de protection de la vie privée et de sécurité	?	Oui	Allemagne	Rewebber	Payant. Abonnement obligatoire. Disponible sur le Web.	Chiffrement. Anonymat/ pseudonymat.	Empêchement de la collecte.	Personnes physiques.
Junkbusters Corporation http://internet.junkbuster.com	Entreprise de protection de la vie privée et de sécurité	1996	Oui	États-Unis	Internet Junkbuster Proxy v. 2.0.2	Gratuit. A installer. Licence : GPL	Filtrage de cookies. Filtrage de la publicité.	Limitation de la collecte/ choix.	Personnes physiques.
KeepItSecret	Entreprise de protection de la vie privée et de sécurité	?	Non	États-Unis (nom de domaine)	KeepItSecret (?)	Gratuit/ payant. Disponible sur le Web. Gratuit avec l'inscription/ envois journaliers, paiement les factures sans envoi	Anonymat/ pseudonymat. Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.
Kookaburra Software www.kburra.com	Entreprise de logiciels	1996	Oui	États-Unis	Cookie Pal v. 1.6	Payant. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Lavasoft www.lavasoftusa.com	Entreprise de logiciels	?	Non	Suède ? États-Unis ?	Ad-Aware, Ad-Aware Plus v. 5.5	Gratuit/ payant. A installer. Gratuit pour la version de base, payant pour les versions avancées	Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Lumeria, Inc. www.lumeria.com	Entreprise de protection de la vie privée, de sécurité et de marketing	1998	Oui	États-Unis	Sunshine technology, comprenant SuperProfile	Outil commercial. Version beta.	Gestion de données personnelles. Filtrage de cookies. Filtrage de la publicité. Gestion du marketing avec consentement. Schéma complexe.	Limitation de la collecte/ choix.	Personnes physiques. Organisations.
MailEncrypt	Entreprise de protection de la vie privée sur Internet	1998	Oui	États-Unis	MailEncrypt	Payant. Abonnement obligatoire. Disponible sur le Web.	Chiffrement. Protection des méls.	Sécurité.	Personnes physiques.
Mailsafe www.mailsafe.org	Entreprise de protection de la vie privée sur Internet	1998	Oui	Gibraltar	Mailsafe	Payant. Abonnement obligatoire. Disponible sur le Web.	Chiffrement. Protection des méls.	Sécurité.	Personnes physiques.
MetaURL Corporation www.idmask.com	Entreprise de protection de la vie privée et de sécurité	?	Oui	Canada	ID Mask	Gratuit/ payant. Abonnement obligatoire. A installer (java). Version gratuit avec largeur de bande restreinte. Abonnement avec largeur de bande non limitée. Code source pourrait être mis dans le domaine public.	Anonymat/ pseudonymat. Filtrage de cookies.	Limitation de la collecte/ choix. Empêchement de la collecte.	Personnes physiques.
Microsoft www.microsoft.com	Entreprise de logiciels	1975	Oui	États-Unis	Internet Explorer 6 (avec quelques éléments P3P et filtrage de cookies) v. 6_PP_Refresh	Gratuit. Beta. version à télécharger gratuitement ou partie de Windows XP	Gestion de données personnelles. Filtrage de cookies.	Limitation de la collecte/ choix. Notification.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
MishkinSoft www.multiproxy.org	Entreprise de logiciels	?	Non	Russie	MultiProxy v. 1.2	Gratuit. A installer. Gratuit pour usage personnel	Anonymat/ pseudonymat.	Empêchement de la collecte.	Personnes physiques.
Naviscope Software www.naviscope.com	Entreprise de logiciels	?	Non	États-Unis (nom de domaine)	Naviscope	Gratuit. A installer. Pourrait devenir payant à l'avenir.	Filtrage de cookies. Filtrage de la publicité.	Limitation de la collecte/ choix.	Personnes physiques.
NetHush	?	2001	Oui	États-Unis (nom de domaine)	NetHush	Gratuit. Disponible sur le Web. Financé par la publicité.	Anonymat/ pseudonymat. Filtrage de cookies. Filtrage de la publicité.	Empêchement de la collecte.	Personnes physiques.
Orangatango www.orangatango.com	Entreprise de protection de la vie privée sur Internet	2000 (droit d'auteur)	Oui	États-Unis	Virtual Browser v. 1.0	Gratuit/payant. Abonnement obligatoire. Disponible sur le Web. Essai d'une semaine gratuit.	Chiffrement. Anonymat/ pseudonymat. Filtrage de la publicité.	Sécurité. Empêchement de la collecte.	Personnes physiques.
Organisation pour la coopération et développement économiques http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm	Organisation internationale	1961	Oui	Siège en France	Générateur de déclarations de politiques de vie privée de l'OCDE	Gratuit. Disponible sur le Web.	Gestion de données personnelles. Didacticiel.	Notification. Didacticiels/ information/ connaissance.	Organisations.
Packetderm, LLC http://freemail.cotse.net/freemail/mail/src/login.php	Entreprise de protection de la vie privée et de sécurité	2000	Oui	États-Unis	Cotse Webmail	Payant. Abonnement obligatoire. Disponible sur le Web. Mél Web gratuit terminé.	Chiffrement. Anonymat/ pseudonymat. Protection des méls.	Sécurité. Empêchement de la collecte.	Personnes physiques.
PC Magazine	Media	?	Oui	États-Unis	CookieCop, CookieCop Plus v. 1.2	Gratuit. A installer. Code source compris.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Persona www.persona.com	Entreprise de protection de la vie privée, de sécurité et de marketing	1998	Oui	États-Unis	p-CRM platform	Payant. Outil commercial.	Gestion de données personnelles. Gestion du marketing avec consentement.	Limitation de la collecte/ choix.	Personnes physiques. Organisations.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
Ponoi Corporation www.ponoi.com	Entreprise de protection de la vie privée et de sécurité	2000 (droit d'auteur)	Oui	États-Unis	Ponoi	A installer (java). Pas d'information sur le modèle commercial. Paraît gratuit.	Chiffrement. Anonymat/ pseudonymat. Contrôle de l'accès.	Sécurité. Empêchement de la collecte.	Personnes physiques.
Potato Software www.skuz.net/potatoware/jbn/about.html	Entreprise de logiciels?	?	Non	?	Jack B. Nymble v. 2	Gratuit. A installer.	Chiffrement. Anonymat/ pseudonymat. Protection des méls.	Sécurité. Empêchement de la collecte.	Personnes physiques.
Privacy Foundation www.bugnosis.org	Groupe de pression	?	Oui	États-Unis	Bugnosis	Gratuit. A installer (ActiveX).	Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
Privacy Software Corporaton www.nsclean.com	Entreprise de protection de la vie privée et de sécurité	1996	Oui	États-Unis	IEClean, NSClean v. 5.5	Payant. A installer.	Filtrage de cookies. Protection des méls.	Limitation de la collecte/ choix.	Personnes physiques.
PrivacyRight www.privacyright.com	Entreprise de protection de la vie privée et de sécurité	?	Oui	États-Unis	TrustFilter (versions spéciales pour les services financiers, les services de santé et le commerce électronique)	Payant. Outil commercial.	Contrôle de l'accès. Audit / conformité. Schéma complexe.	Sécurité. Limitation de la collecte/ choix. Notification. Limitation de l'usage. Accès.	Organisations.
PrivacyX.com Solutions	Entreprise de protection de la vie privée et de sécurité	1998	Oui	Canada	PrivacyX, PremiumX	Gratuit/ payant. Disponible sur le Web. Service sur le Web gratuit, mais comporte de la publicité (privacyX) ; version plus avancée payante et sans publicité (PremiumX). Utilisateur doit installer un certificat et peut utiliser son programme de mél habituel.	Anonymat/ pseudonymat. Contrôle de l'accès.	Sécurité. Empêchement de la collecte.	Personnes physiques.
Rendering Better Avenues Software www.rbaworld.com	Entreprise de logiciels	1997 (droit d'auteur))	Non	États-Unis (nom de domaine)	Cookie Cruncher v. 2.11	Gratuit. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
SafeWeb www.safeweb.com	Entreprise de protection de la vie privée et de sécurité	2000	Oui	États-Unis	SafeWeb Triangle boy	Gratuit. Disponible sur le Web/ A installer. Disponible sur le Web for SafeWeb, A installer pour Triangle boy	Anonymat/ pseudonymat. Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix. Empêchement de la collecte.	Personnes physiques.
SendFakeMail www.sendfakemail.com	Entreprise de protection de la vie privée et de sécurité	?	Non	Thaïlande	SendFakeMail	Payant. Abonnement obligatoire. Disponible sur le Web.	Anonymat/ pseudonymat. Protection des méls.	Sécurité. Empêchement de la collecte.	Personnes physiques.
SiegeSoft	Entreprise de protection de la vie privée et de sécurité	1998	Oui	Canada	Siege Surfer	Payant. Abonnement obligatoire. Disponible sur le Web.	Anonymat/ pseudonymat. Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.
Spyblocker Software www.morelerbe.com/spyblocker	Entreprise de logiciels	?	Oui	États-Unis	SpyBlocker v. 4.2	Gratuit. A installer.	Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware.	Limitation de la collecte/ choix.	Personnes physiques.
SpyChecker.com www.spychecker.com	Groupe de pression ?	?	Oui	États-Unis	SpyChecker v. 1.1	Gratuit. Disponible sur le Web/ A installer.	Filtrage de spyware.	Notification.	Personnes physiques.
The Cloak www.the-cloak.com/anonymous-surfing-home.html	?	?	Oui	?	The Cloak	Gratuit. Disponible sur le Web.	Anonymat/ pseudonymat. Filtrage de cookies.	Empêchement de la collecte.	Personnes physiques.
The Limit Software www.thelimitsoft.com	Entreprise de logiciels	1994	Oui	États-Unis	Cookie Crusher v. 2.6	Payant. A installer.	Filtrage de cookies.	Limitation de la collecte/ choix.	Personnes physiques.
Watchfire www.watchfire.com	Entreprise de technologies Internet	1996	Oui	Canada	WebCPO	Payant. Outil commercial.	Audit/ conformité.	Responsabilité.	Organisations.
World Wide Web Consortium www.w3.org	Consortium industriel	1994	Oui	International	Platform for Privacy Preferences (P3P) v. 1.0	A incorporer dans les navigateurs et sur les sites Web des organisations.	Gestion de données personnelles.	Limitation de la collecte/ choix. Notification.	Personnes physiques. Organisations.

Nom de l'organisation et adresse Internet	Type d'organisation	Date de l'établissement de l'organi-sation	Politique de protection de la vie prive sur le site	Origine géographique	Nom et version des principaux produits pets	Caractéristiques du produit	Fonctionnalité principale	Impact au regard des principes de protection des données	Audience principalement visée
YOUPowered	Entreprise de protection de la vie privée, de sécurité et de marketing ? ?	?	Oui	États-Unis	Orby v. 3.0 beta	Gratuit. A installer. Version beta.	Gestion de données personnelles. Filtrage de cookies. Filtrage de spyware. Contrôle de l'accès.	Limitation de la collecte/ choix. Notification.	Personnes physiques.
YOUPowered	Entreprise de protection de la vie privée, de sécurité et de marketing ? ?	?	Oui	États-Unis	SmartPrivacy Publisher	Payant. A installer.	Gestion de données personnelles.	Notification.	Organisations.
Zero Knowledge www.zeroknowledge.com	Entreprise de protection de la vie privée et de sécurité	1997	Oui	Canada	Freedom Internet Privacy Suite v. 2.0	Gratuit/ payant. A installer. Gratuit pour la version standard/ payant pour la version améliorée.	Anonymat/ pseudonymat. Filtrage de cookies. Filtrage de la publicité. Filtrage de spyware. Protection des méls.	Sécurité. Limitation de la collecte/ choix. Empêchement de la collecte.	Personnes physiques.
ZipLip, Inc www.ziplip.com	Entreprise de protection de la vie privée et de sécurité	1999	Oui	États-Unis	ZipLip Plus	Gratuit. Inscription obligatoire. Disponible sur le Web.	Chiffrement. Anonymat/ pseudonymat. Protection des méls.	Sécurité. Empêchement de la collecte.	Personnes physiques.

APPENDICE II. PEUT-ON NOUS FAIRE APPRIVOISER LES TECHNOLOGIES PROTECTRICES DE LA VIE PRIVÉE PAR LA PERSUASION ?[1]

Introduction

Au cours des 15 dernières années, les responsables de la réglementation en matière de protection des données, les milieux technologiques intéressés par la protection de la vie privée et d'autres intervenants ont élaboré le concept de technologies protectrices de la vie privée[2] (TPVP) et les outils qui y sont associés.

On peut entendre par « technologies protectrices de la vie privée » les systèmes numériques utilisés par les produits et services, et intégrés à ceux-ci, qui visent à limiter les risques d'atteinte à la vie privée et permettent aux personnes concernées d'exercer leurs droits en matière de respect de la vie privée, notamment les technologies qui tentent de contrôler le traitement de l'information à caractère personnel pour réduire les risques de traitement non justifié, par exemple, en assurant le respect de l'anonymat ou du pseudonymat souhaité, en permettant aux personnes concernées d'exprimer leurs préférences quant à l'utilisation de leur information, d'obtenir un accès sécurisé aux renseignements détenus à leur sujet et de donner leur consentement à la collecte ou au traitement de données les concernant, et en limitant le type de données collectées, les modalités de leur divulgation ou les systèmes auxquels elles peuvent être divulguées[3]. J'avance pour ma part une définition plus large que celles de certains auteurs : en effet, je ne limite pas les TPVP aux outils qui assurent le pseudonymat, ni ne fais ici de distinction entre outils de « renforcement de la protection de la vie privée » et outils de « protection de la vie privée ». J'utilise un seul terme pour parler des deux réalités. A point nommé, j'exposerai une classification (voir figure 3). Jusque là, cependant, l'expression « technologie

---

1. Cette étude a été réalisée par M. Perri 6, Directeur du *Policy Programme* de l'*Institute for Applied Health and Social Policy*, au *King's College* de Londres, en qualité de consultant auprès de l'OCDE. L'auteur exprime ses remerciements à Mme Anne Carblanc, de l'OCDE, qui lui a commandé cette étude, ainsi qu'à cette dernière, à Charles Raab, Phil Boyd, Brendon Swedlow, James Tansey et Mary Culnan pour leurs commentaires sur une version antérieure de l'étude. L'auteur précise que ces personnes ne souscrivent pas nécessairement à ses arguments et que l'on ne saurait leur imputer quelque responsabilité que ce soit pour ses erreurs éventuelles.

2. Commissaire à l'information et à la protection de la vie privée, Ontario (Canada) et Registratiekamer (Pays-Bas), 1995, Privacy enhancing technologies: the path to anonymity, vols I and II.. Voir également Registratiekamer (Pays-Bas), 1999, Intelligent software agents: turning a privacy threat into a privacy protector, Commissaire à l'information et à la protection de la vie privée, Ontario (Canada) et Registratiekamer (Pays-Bas), Toronto et Rijkswijk. Voir également la typologie établie dans Burkert H. 1997, « Privacy enhancing technologies: typology, critique, vision », dans Agre P.E. et Rotenberg M., (dir. publ.), 1997, Technology and privacy: the new landscape, Massachusetts Institute of Technology press, Cambridge (Massachusetts) pp. 125-142.

3. Voir la description générale donnée dans Burkert H, 1997, « Privacy enhancing technologies: typology, critique, vision », dans Agre P.E. et Rotenberg M., (dir. publ.), 1997, *Technology and privacy: the new landscape*, Massachusetts Institute of Technology press, Cambridge (Massachusetts) pp. 125-142.

protectrice de la vie privée » est à considérer comme l'un des vocables désignant la pléthore de dispositifs de sécurité qui se multiplient dans tous les secteurs, depuis l'industrie chimique et les centrales nucléaires jusqu'au transport aérien[4].

Toutes les parties prenantes susmentionnées veulent maintenant savoir s'il est possible de persuader les entreprises d'investir dans les TPVP et de convaincre les consommateurs d'exiger ces technologies. A ce jour, d'après l'information dont nous disposons sur le nombre de cyberentreprises qui proposent aujourd'hui ne serait-ce que les précautions les plus élémentaires en matière de protection de la vie privée, telles que fournir de l'information sur la collecte, l'utilisation et la divulgation de l'information, offrir aux consommateurs un choix quant à l'information qu'ils veulent révéler ou à sa divulgation, ou encore l'accès de la personne concernée aux données, seule une minorité d'entreprises ont fait les modestes investissements nécessaires[5]. Quant à la proportion d'entreprises offrant le pseudonymat, elle est certainement beaucoup plus faible. En effet, dans une recherche universitaire dont les résultats seront publiés prochainement, on a utilisé un ordinateur personnel équipé du nouveau logiciel Internet Explorer 6, y compris le système de définition des préférences en matière de vie privée P3P, pour visiter un certain nombre de sites Web commerciaux. L'étude a permis de constater que les logiciels de nombreux sites de l'échantillon avaient demandé au chercheur d'ajuster à la baisse ses critères en matière de protection de la vie privée pour pouvoir utiliser le site[6]. Voilà qui tend à montrer que si les gouvernements veulent que les TPVP soient plus largement utilisées, ils ont un travail de persuasion à faire.

J'utilise ici le mot « persuasion » tout en sachant pertinemment qu'il est indélicat. Jusqu'ici en effet, l'OCDE a préféré – on le comprend – parler d'« éducation » ou de « sensibilisation », termes qui évoquent beaucoup moins l'intrusion ou la manipulation. Car même si nous vivons à une époque où

---

4. De fait, ces technologies susciteront immanquablement, en temps voulu, bon nombre des mêmes questions que celles qui se posent au sujet des dispositifs de sécurité : fonctionnent-ils, sont-ils susceptibles de favoriser la complaisance ou d'affaiblir la vigilance, augmentent-ils la complexité au point d'induire finalement des atteintes à la vie privée ? Pour l'essentiel de l'argumentation selon laquelle l'intégration de caractéristiques visant à réduire les risques dès la conception des systèmes accroît la complexité et peut aboutir à des dérives, voir Perrow C., 1999 [1984], *Normal accidents: living with high risk technologies*, 2ème édition, Princeton University Press, Princeton, (New Jersey). Pour un développement récent de l'argument selon lequel la multiplication des systèmes visant à réduire les risques favorise chez les gens une certaine complaisance à l'égard du risque, voir Adams J, 1995, *Risk*, UCL Press, Londres. En ce qui concerne le principal développement de l'argument selon lequel l'intégration, à l'étape de la conception des produits, de caractéristiques visant à réduire les risques aboutit à des systèmes inflexibles qui augmentent souvent la probabilité des risques mêmes que ces caractéristiques ont pour but de réduire, voir Wildavsky A., 1988, *Searching for safety*, Transaction Publishers, New Brunswick (New Jersey). Du reste, le raisonnement de Burkert fait ressortir la possibilité que des atteintes à la vie privée se produisent dans des systèmes utilisant ces technologies pour chacune de ces raisons, bien qu'il ne fasse pas l'analogie avec les recherches sur la gestion des risques en général. Burkert H, 1997, « Privacy enhancing technologies: typology, critique, vision », dans Agre P.E. et Rotenberg M., (dir. publ.) 1997, *Technology and privacy: the new landscape*, Massachusetts Institute of Technology press, Cambridge, (Massachusetts), pages 125-142.

5. Federal Trade Commission, 2000, *Privacy online: fair information practices in the electronic marketplace: a Federal Trade Commission report to Congress*, mai, Federal Trade Commission, Washington DC, accessible sur www.ftc.gov/reports/privacy2000/privacy2000text.pdf. Voir également Consumers International, 2001, *Privacy@net: an international comparative study of consumer privacy on the internet*, Consumers International, Londres, disponible sur www.consumersinternational.org/news/ pressreleases/fprivreport.pdf.

6. Cette recherche est actuellement menée au département de gestion et de technologie de l'information du Bentley College (Massachusetts) ; Mary Culnan, communication personnelle, 3 octobre 2001.

l'on estime que l'art et les moyens de persuader ont atteint des sommets d'efficacité – et sans doute en partie précisément *pour cette raison* –, il est aujourd'hui jugé inconvenant d'admettre que la communication, l'éducation, la formation, la fourniture d'information et même la publicité relèvent purement et simplement de la persuasion. Néanmoins, s'agissant de contribuer à la réflexion de l'OCDE sur la question de savoir quand, à l'égard de qui et dans quelles circonstances la « communication » au sujet des TPVP peut produire des résultats et favoriser une plus grande ouverture à leur utilisation, on ne saurait feindre d'ignorer que c'est bel et bien de persuasion et d'influence qu'il s'agit. De fait, bon nombre des travaux sur lesquels s'appuie la présente étude portent explicitement sur la persuasion. Une discussion de l'éventail des formes et stratégies plus ou moins intrusives et plus ou moins manipulatrices de la persuasion dépasserait le cadre qui m'est ici imparti. Cependant, il convient de noter que ceux qui ont étudié la propagande sous diverses formes sont en général parvenus à la conclusion que les stratégies les plus manipulatrices et les plus insidieuses sont souvent inopérantes, qu'elles n'ont en général d'effet qu'à court terme, et qu'à mesure que leur vraie nature se fait jour, elles s'affaiblissent d'elles-mêmes[7]. L'objet de mon étude est donc de voir dans quelle mesure les moyens les plus honnêtes d'influencer les cœurs et les esprits peuvent être mis en œuvre pour stimuler la motivation à utiliser les TPVP.

Mon argument est que tout le monde ne pourra pas être facilement persuadé de quelque chose, et encore moins de n'importe quoi, mais que nous pouvons en revanche avoir certaines indications sur qui serait plus susceptible d'être persuadé de quelque chose en particulier, et dans quelles circonstances, de même que nous pouvons également avancer certaines idées – quoique cette fois avec un peu plus de modestie – sur la façon dont des personnes se trouvant dans des situations différentes pourraient être persuadées de choses dont elles seraient susceptibles d'être persuadées. Cependant, il est indispensable de classifier et de segmenter les populations d'entreprises et de consommateurs pour comprendre ce que l'on peut obtenir comme résultat auprès de gens qui se trouvent dans des situations différentes. C'est là, je le sais, une conclusion agaçante pour ceux qui privilégient une optique plus « battante ». Depuis la série télévisée *Yes, Prime Minister*, tous les hauts fonctionnaires s'efforcent d'éviter de donner un avis qui puisse rappeler un tant soit peu la célèbre phrase de Sir Humphrey (« *It's all very complicated, Prime Minister* » – Tout cela est très compliqué M. le Premier Ministre). Malheureusement, il arrive que les choses soient, effectivement, très compliquées. Je vais toutefois tenter de simplifier et de montrer qu'il existe une certaine hiérarchie dans la complexité des conditions qui détermine qui peut être persuadé de quoi.

A mon avis, contrairement à l'opinion dominante des psychologues à orientation moins sociale qui ont dominé le débat sur la persuasion politique et commerciale depuis un siècle, l'examen des facteurs mentaux ne nous sera pas très utile. Cette approche ne sert en effet guère plus qu'à décrire le type de problème à appréhender. Au contraire, mon argument sera que, pour reprendre l'expression d'une des plus grandes études réalisées sur le thème « qui persuade qui, pourquoi et comment » au cours des cinquante dernières années, « tout dépend de la place qu'on occupe »[8]. Autrement dit, la sensibilité à la persuasion – la « persuasibilité » – des entreprises et des consommateurs s'explique dans une large mesure par leur situation, car c'est le contexte institutionnel dans lequel se trouve une

7. Jowett G.S. et O'Donnell V., 1999, *Propaganda and persuasion*, 3ème édition, Sage, Londres, p. 171.

8. Allison G.T., 1971, *Essence of decision: explaining the Cuban missile crisis*, Little, Brown, Boston: voir Allison G.T. et Zelikow P, 1999, *Essence of decision: explaining the Cuban missile crisis*, 2ème édition, Addison Wesley Longman, New York, p. 307. Cette maxime est attribuée à Rufus Miles, un administrateur fédéral des États-Unis pendant les années 60 qui a géré un certain nombre d'agences du programme « *Great Society* » dans l'administration Johnson, et a travaillé au Bureau exécutif du Président et au Bureau du budget. C'est ainsi qu'on parle de la *Miles' Law* (la loi de Miles) : voir Stillman R., 1999, « Where you stand depends on where you sit », *American review of public administration*, 29, 1, pp. 92-97.

personne qui détermine l'information que celle-ci sera capable d'entendre, d'accepter et d'utiliser ou, au contraire, de rejeter[9]. Par ailleurs, une simple stratégie consistant à offrir des incitations pour rendre les gens plus sensibles à la persuasion ne serait pas non plus suffisante et du reste, comme je le note ci-après, de nombreux économistes le reconnaissent aujourd'hui. Les mesures incitatives peuvent avoir leur place, mais tout le monde ne s'entend pas sur ce qu'est une incitation, ou tout au moins une incitation valable.

La structure de l'étude est très simple. Dans la prochaine section, je commencerai par définir brièvement la nature du problème à résoudre, puis dans les deux sections de substance suivantes, je traiterai de la sensibilité, d'abord des entreprises, puis des consommateurs, à la persuasion visant à les inciter, respectivement, à offrir et à réclamer des services dans lesquels sont utilisées ou intégrées des TPVP. Dans chacune de ces sections, je procède de la même façon. Je commence par proposer une segmentation des populations d'entreprises et de consommateurs selon des critères pertinents. L'analyse de la segmentation sert ensuite à identifier les types de protection de la vie privée qui devraient présenter le plus grand intérêt dans chaque segment. Pour chacun, une brève sous-section examine ensuite les moyens par lesquels peut s'exercer la persuasion nécessaire. Ces deux éléments centraux de l'argumentation sont suivis, dans une section finale, d'une discussion de fond qui montre que les approches de base utilisées à l'égard des entreprises et des consommateurs ne sont pas seulement compatibles, mais en fait identiques dans leur structure sous-jacente, même si cela n'était peut-être pas évident a priori. Cela permet de procéder à l'examen de la dynamique de l'intérêt que suscite les TPVP et du degré de persuasibilité à l'égard de ces technologies, examen pour lequel je situe consommateurs et fournisseurs dans un même cadre. Enfin, dans une brève section de conclusion, je résume les principaux enseignements à tirer pour les responsables de l'action gouvernementale qui veulent tenter de persuader les entreprises et les consommateurs de s'intéresser davantage aux TPVP.

La structure du problème de la persuasion et ce que nous devons apprendre

Pour offrir aux consommateurs des produits et services dont la conception intègre des TPVP, les entreprises doivent investir, et elles ne seront prêtes à en assumer le coût que si elles jugent l'investissement suffisamment rentable. L'ajout de TPVP aux systèmes informatiques en place entraîne souvent, mais bien entendu pas toujours, une augmentation des coûts unitaires. Cette augmentation peut être beaucoup plus faible pour les nouveaux produits dont la conception intègre les TPVP « à la source ». Si les entreprises craignent de ne pas pouvoir répercuter ces coûts additionnels sous forme de prix plus élevés, elles craindront également que leurs concurrents ne soient capables de les évincer en offrant des services et des systèmes moins chers et n'intégrant pas de TPVP. Les avantages directs de la protection de la vie privée reviennent aux consommateurs (et peut-être à des publics plus larges), pas aux entreprises. Pour ces dernières, les avantages sont en effet indirects. Le problème qui se pose lorsqu'on veut persuader les entreprises d'investir dans les TPVP est donc un problème classique, comme lorsqu'on tente de les inciter à adopter un comportement éthique ou des pratiques respectueuses de l'environnement. Pour le formuler en termes économiques, on peut dire que le problème consiste à persuader les entreprises qu'elles devraient internaliser certains coûts qu'elles ont été capables d'externaliser, alors que les conditions de concurrence pourraient – tout au moins dans de nombreux marchés – favoriser justement celles qui externalisent par rapport à celles qui

9. Douglas M., 1986, *How institutions think*, Routledge and Kegan Paul, Londres; Thompson M. et Wildavsky A., 1986, « A cultural theory of information bias in organizations », *Journal of management studies*, 23, 3, pp. 273-286.

internalisent[10]. Il ne s'agit pas, comme je vais le montrer, d'un problème forcément insoluble, mais d'un problème qui est effectivement complexe et auquel n'existe qu'un nombre fini de types de réponses. Cependant, pour apprendre quelque chose au sujet de ces types de réponses possibles, nous pouvons examiner les enseignements qui se dégagent des tentatives visant à influencer les entreprises pour leur faire adopter des technologies respectueuses de l'environnement ou diverses pratiques dites « éthiques », et déterminer si certains peuvent s'appliquer à la situation des TPVP.

Pour éviter de donner trop d'ampleur à la présente étude, je laisserai de côté le problème que pose la persuasion à exercer sur les organismes publics – qu'ils soient prestataires de services ou acheteurs de services auprès du secteur privé – pour leur faire intégrer les TPVP à leurs cahiers des charges[11].

---

10. Pour une réflexion sur les facteurs économiques à prendre en compte pour inciter les entreprises à internaliser les coûts qu'elles pourraient externaliser et dont elles pourraient craindre que d'autres ne les externalisent, voir Baumol W.J., avec Blackman S.A.B., 1991, *Perfect markets and easy virtue: business ethics and the invisible hand*, Blackwell, Oxford, *passim* mais surtout chapitre 3. Certains prétendront que le problème consiste à faire en sorte que les entreprises internalisent les coûts de fourniture de biens publics. J'évite de poser le problème de cette façon, pour deux raisons. D'abord, il y a débat pour déterminer dans quelle mesure la protection de la vie privée peut être considérée comme un bien public, et jusqu'à quel point le caractère divisible de la gestion de l'information à caractère personnel fait de celle-ci un bien privé. Voir par exemple Spinello R.A., 1998, « Privacy rights in the information economy: review of Legislating privacy: technology, social values and public policy, Priscilla Regan, Chapel Hill: UNC Press, 1995 », *Business ethics quarterly*, 8, 4, pp. 723-742. Je n'ai pas l'intention d'entrer ici dans ces considérations ésotériques. Ensuite, la question de savoir ce qui entre dans la catégorie des biens publics et des biens privés dépend également de la situation dans laquelle on se trouve : Voir Wildavsky A., dans Wildavsky A., (dir. publ.) par Chai S-K et Swedlow B, 1998, « At once ubiquitous and elusive, the concept of externalities is either vacuous or misapplied », dans Wildavsky A., 1998, *Culture and social theory*, Transaction Publishers, New Brunswick, (New Jersey), pp. 55-84. Quoi qu'il en soit, l'argument peut être invoqué sans les hypothèses retenues ici, et l'utilité de l'analogie entre les TPVP et les technologies de protection de l'environnement ou l'éthique commerciale ne dépend pas de la formulation de ces hypothèses relatives aux externalités et aux biens publics.

11. On pourrait supposer, dans l'optique de la présente étude, que le problème peut être résolu par des moyens administratifs, tels que la directive ou le règlement interne au sein de l'appareil public. Dans la pratique, les choses ne sont toutefois pas aussi simples, comme l'ont montré deux générations de recherche sur la mise en œuvre. Cependant, l'expérience du *British National Health Service* depuis le rapport du Comité Caldicott fournira une étude de cas précieuse qui servira à tester les assertions contradictoires concernant l'efficacité de la direction administrative en tant que stratégie visant à assurer la conformité aux règles de protection de la vie privée dans le secteur public : voir Ministère de la santé, 1997, *The Caldicott Committee report on the review of patient-identifiable information*, Ministère de la santé, Londres ; voir également les lignes directrices et rapports subséquents sur la mise en œuvre, qui sont accessibles sur www.doh.gov.uk/nhsexipu/confiden/. Il est encore trop tôt pour évaluer les enseignements à tirer de cette expérience. Dans la pratique, bon nombre des considérations qui s'appliquent à la persuasibilité des entreprises valent également pour les organismes publics, à quelques différences complexes près qui ne peuvent être examinées ici. Pour un aperçu des contraintes et des incitations qui font que le personnel de première ligne n'internalise pas les coûts que l'élément central pourrait vouloir qu'il internalise, voir Lipsky M., 1980, *Street level bureaucracy: dilemmas of the individual in public services*, Russell Sage Foundation, New York. Sur les aspects généraux des problèmes de mise en œuvre dans la situation où l'on a recours à l'orientation administrative pour pousser les organismes subalternes à internaliser les coûts, voir Bardach E., 1977, *The implementation game*, Massachusetts Institute of Technology Press, Cambridge, (Massachusetts). Le lecteur qui s'intéresse aux difficultés que pose l'utilisation des règlements internes, consultera par exemple Hood C., Scott C., James O., Jones G. et Travers T., 1999, *Regulation inside government: waste-watchers, quality police and sleaze-busters*, Oxford University Press, Oxford. En théorie tout au

Si l'on tente maintenant de cerner la tâche délicate qui consiste à persuader les consommateurs d'exiger les TPVP, c'est par les préférences de ces derniers qu'il faut commencer. En effet, tous les consommateurs n'ont pas le même souci de protéger leur vie privée : il en est qui attachent plus d'importance à certains risques qu'à d'autres, certains ont davantage confiance que d'autres dans l'efficacité de la protection technologique de la vie privée, ou font plus confiance à certaines technologies qu'à d'autres. Autrement dit, la première chose qu'il faut comprendre, c'est comment la population de consommateurs se répartit selon sa *perception* des divers risques d'atteinte à la vie privée. C'est donc la reconnaissance des risques qui est à l'origine du désir des consommateurs de se protéger. De plus, afin de comprendre les possibilités de persuasion, il faut savoir dans quelle mesure les perceptions des risques d'atteinte à la vie privée peuvent être influencées ou modifiées.

Dans un marché où le prix des produits et services dans lesquels sont incorporés les TPVP est plus élevé que celui des prix dépourvus de ces technologies (hypothèse pessimiste que nous pouvons aisément retenir pour élargir l'utilité de l'argument), le consommateur doit décider de la valeur qu'il attribue aux types de protection de la vie privée que le service lui offre, par rapport à l'importance et au coût véritables de l'écart de prix. La deuxième chose qu'il nous faut apprendre au sujet des consommateurs c'est comment se fait l'arbitrage entre d'une part leurs préférences en matière de protection contre divers types de risques d'atteinte à la vie privée et d'autre part les augmentations de prix. Si cet arbitrage peut être influencé, on peut alors présumer (à moins que quelqu'un ne propose une nouvelle idée pour accroître les niveaux de revenu à affectation libre des consommateurs sans entraîner d'inflation correspondante !), que la seule façon de persuader les gens de consentir à payer davantage pour protéger leur vie privée est de faire en sorte, d'abord, qu'ils attachent plus d'importance aux risques d'atteinte à la vie privée.

Dans l'éventualité peu probable où le marché serait parfaitement concurrentiel et où les consommateurs auraient, pour ainsi dire, la possibilité de trouver de nouveaux fournisseurs et d'en changer sans surcoût, les consommateurs se répartiraient selon leurs préférences et leur consentement à payer des biens et services, en fonction de l'arbitrage entre la « qualité » et le prix de la protection de la vie privée qu'ils seraient prêts à faire à l'aide de l'information qu'ils seraient capables (dans un marché parfaitement concurrentiel) de se procurer à un coût négligeable sur les caractéristiques de protection de la vie privée des services concurrents. Dans la réalité, il existe certes sur de nombreux marchés des coûts réels pour les consommateurs qui veulent chercher, obtenir et vérifier de l'information, et exercer leur capacité de mobilité entre les fournisseurs – sans compter qu'il peut y avoir une situation d'oligopole ou d'autres limites à l'éventail de services disponibles, et que les entreprises peuvent proposer des renseignements trompeurs quant aux caractéristiques de protection de la vie privée de leurs services. La troisième chose enfin qu'il nous faut apprendre, c'est comment les consommateurs évaluent les *coûts de transaction* – qui ne peuvent pas tous être monétisés, mais que l'on peut exprimer en termes de temps perdu – liés à la recherche, à la vérification et à la mobilité.

---

moins, si les organismes du secteur public offraient des services assurant un meilleur respect de la vie privée et faisant davantage appel aux TPVP, les attentes des consommateurs pourraient devenir plus grandes, de même que leur familiarité avec ces technologies, ce qui pourrait se répercuter sur leur comportement à l'égard des entités commerciales avec lesquelles ils traitent. Les marchés de services passés par les organismes publics avec le secteur privé pourraient également avoir une influence du côté de l'offre. Cependant, l'expérience antérieure, s'agissant par exemple des pratiques en matière d'égalité des chances dans le secteur public, porte à croire que la prudence serait de mise en ce qui concerne la rapidité et l'ampleur de ces retombées, ainsi que leur résistance aux chocs et leur capacité de vaincre la résistance des pressions commerciales et institutionnelles exercées dans le sens contraire.

Persuader les entreprises

Pourquoi les entreprises devraient-elles internaliser des coûts qu'elles pourraient externaliser et dont elles peuvent craindre que leurs concurrents les externalisent si elles les internalisent ? En général, on peut retenir quatre types de situations de base dans lesquelles les entreprises peuvent avoir des raisons d'agir ainsi. Ces situations peuvent être regroupées en deux catégories générales. La première comprend les situations dans lesquelles les entreprises sont exposées à des *sanctions* et bénéficient *d'incitations* pour internaliser ces coûts, la seconde correspond aux situations où les entreprises sont soumises à des *contraintes* qui font qu'il leur est difficile d'envisager de ne pas internaliser les coûts en question.

Sanctions et incitations

1. *La crainte :* Il existe des situations où les entreprises craignent, si elles n'internalisent pas les coûts et n'investissent pas dans les TPVP, de faire l'objet de sanctions de la part du régulateur. Si les TPVP sont régies par des normes établies par des organismes nationaux et internationaux, par exemple, les entreprises adopteront ces normes car elles signaleront ainsi au régulateur qu'elles se comportent conformément à ses exigences et qu'elles adhèrent aux valeurs qu'il défend.

2. *L'espoir :* Dans cette situation, au moins certains groupes de consommateurs revêtant une importance pour les entreprises exigent que les TPVP soient intégrées à la conception des services et produits. C'est pourquoi des investissements dans les TPVP peuvent constituer pour une entreprise un avantage concurrentiel pour attirer la clientèle de ces groupes de consommateurs. Dans un tel cas, l'adoption des normes relatives aux TPVP a fonction de signal à l'intention de ces groupes de consommateurs et contribue à construire une réputation auprès de ces derniers.

Contraintes

1. *L'habitude :* Dans cette situation, pour les entreprises d'un secteur ou d'un segment donné, l'utilisation des TPVP est devenue la norme et, indépendamment de toute incitation ou sanction, ces technologies seront adoptées et leurs coûts internalisés car cela constitue pour tous les concurrents la règle implicite. Les technologies ne sont plus considérées comme une question à part. Cette habitude, assimilée par les entreprises, limite en soi les possibilités d'envisager de ne pas utiliser les TPVP.
2. *Impossibilité de faire autrement :* Les TPVP sont incorporées dans d'autres produits et services qui doivent être utilisés car il n'existe pas d'autre possibilité que d'en utiliser au moins une. Par exemple, des normes de produits pourraient exiger l'utilisation de TPVP universellement adoptés. En général, c'est ce qui se produit lorsque l'évolution technologie fait que certaines technologies, indépendamment de tout avantage concurrentiel ou de pression réglementaire, parviennent à s'imposer de façon définitive. Autrement dit, l'utilisation d'autres systèmes devient impossible en partie parce que les attentes, de même que les coûts d'un éventuel changement pour les entreprises et les consommateurs sont devenus trop importants, parce que la technologie en question s'est solidement institutionnalisée et que l'infrastructure qui s'y rattache est parfaitement établie[12].

12. Arthur B., 1990, « Positive feedbacks in the economy », *Scientific American*, février, pp. 92-99; Rosenberg N., 1994, *Exploring the black box: technology, economics and history*, Cambridge

Pour les besoins de la présente étude, nous devons – malheureusement – laisser de côté l'habitude et l'impossibilité de faire autrement, car comme l'ont montré les études historiques sur l'imposition définitive du clavier AZERTY et du moteur à combustion interne, il n'existe aucun itinéraire direct vers l'habituation ou l'omniprésence définitive d'une technologie qui ne passe au préalable par les pressions dynamiques de l'espoir et de la crainte. Toutes les habitudes et toutes les innovations sont à un moment ou un autre *nouvelles*, et pour survivre aux « aléas de la nouveauté », elles doivent être adoptées de façon explicite, d'emblée et sur la base d'un certain équilibre entre espoir et crainte.

Cependant, les situations dans lesquelles l'espoir et la crainte peuvent motiver l'internalisation des coûts que les concurrents pourraient externaliser ne sont pas universelles et se retrouvent plutôt dans des types de secteurs très distincts. Pour les mêmes raisons qu'en ce qui concerne leur répartition particulière, associer espoir et crainte n'est pas chose facile, tant s'en faut.

Considérons d'abord les situations dans lesquelles la crainte des sanctions réglementaires est le plus susceptible d'être efficace. C'est bien sûr dans les secteurs de l'économie qui se prêtent le plus à la réglementation que les régulateurs obtiennent les meilleurs résultats. Il s'agit en général des secteurs les plus stables, car il est très coûteux pour les régulateurs d'obtenir de l'information sur des comportements de profiteurs reposant sur l'exploitation de la vie privée des consommateurs dans des secteurs très changeants et où la concurrence est très vive[13]. En outre, dans les marchés et secteurs où les entreprises apparaissent, disparaissent et réapparaissent sous de nouvelles formes à un rythme effréné, les régulateurs ont fort à faire.

Dans les secteurs du marché où les consommateurs ne peuvent pas facilement savoir si leur vie privée est respectée, peut-être parce qu'ils ne savent pas que les industries en question possèdent beaucoup d'informations les concernant (ou que certains types de renseignements les concernant ont en fait une grande valeur, car ils peuvent être très utiles pour déduire d'autres types de renseignements), les entreprises ont beaucoup d'autres possibilités d'exploiter sans scrupules l'information à caractère personnel à l'insu des régulateurs, qui s'en remettent souvent aux consommateurs pour les alerter en cas de violation.

Les marchés et secteurs varient du point de vue des arrangements institutionnalisés qui existent pour le partage d'informations sur ce qui vaut aux entreprises et à leurs hauts dirigeants une bonne ou une mauvaise réputation. Les secteurs dépourvus de ce genre de système institutionnalisé de partage d'informations offrent davantage de possibilités aux entreprises peu scrupuleuses d'échapper au bras du régulateur, qui n'est de toute façon pas si long.

Les caractéristiques économiques des marchés ne sont néanmoins pas les seules à déterminer la facilité avec laquelle peut s'exercer la réglementation. Le degré d'attention des groupes de pression, notamment de ceux qui représentent les consommateurs pour les questions de protection de la vie privée, a également son importance. Les industries vers lesquelles ces groupes choisissent de mobiliser leurs ressources limitées sont par conséquent plus faciles à réglementer, car les groupes de pression assument une partie des coûts d'obtention de l'information qui devraient autrement être pris en charge par les régulateurs.

University Press, Cambridge; David P.A., 1985, « Clio and the economics of QWERTY », *Economic history*, 75, 2, pp. 332-337; Pool R., 1997, *Beyond engineering: how society shapes technology*, Oxford University Press, New York, ch.5.

13. Au sujet de l'asymétrie de l'information entre régulateur et réglementé en faveur du second, voir Klein R.E. et Day P., 1987, « The regulation of nursing homes », *Milbank quarterly*, 65, 3, pp. 303-347.

Les caractéristiques institutionnalisées internes des entreprises ont également une grande influence. En effet, les entreprises dont les dirigeants souscrivent aux principes du respect de la vie privée des consommateurs seront plus susceptibles de se doter de contrôles institutionnalisés pour veiller à l'intégration des TPVP, de soutenir ceux qui tirent la sonnette d'alarme en cas de violation, et de se montrer coopératives lorsque les autorités réglementaires leur demanderont de l'information. Ces caractéristiques institutionnalisées ne sont cependant pas réparties de façon aléatoire. En effet, l'adhésion à de tels contrôles fera son apparition lorsque cela sera justifié, en fonction du contexte, et notamment du créneau[14].

S'agissant maintenant des secteurs dans lesquels des stratégies tablant sur l'espoir pourraient être efficaces pour inciter les entreprises à investir dans les TPVP, l'espoir réside essentiellement dans la demande de consommation, sur laquelle nous nous pencherons plus longuement dans la prochaine section. Cependant, quelle que soit la façon dont on aborde les différences qui existent entre les consommateurs en ce qui concerne l'importance qu'ils attachent à la protection de la vie privée en général, et à la protection contre différents risques d'atteinte à la vie privée en particulier, on s'accorde en général à reconnaître que certains consommateurs ont des préférences qui peuvent faire que les entreprises, s'il est rentable pour elles d'attirer ces consommateurs, pourront être plus facilement persuadées que dans d'autres circonstances du bien-fondé des investissements dans les TPVP. Les questions clés qui se posent dans le cadre des stratégies fondées sur l'espoir sont les suivantes : quelle est la taille de la population de consommateurs qui souhaitent l'un ou l'autre des types de TPVP disponibles, combien de consommateurs parmi eux sont prêts à payer et combien en coûtera-t-il aux entreprises pour les attirer ?

Le domaine de la consommation écologique peut fournir ici une analogie utile. En effet, les études sur la tendance à l' « écoconsommation » – adoption du compostage des déchets organiques ménagers, recyclage, consommation de café et de thé issus du « commerce équitable », emballage minimal, volonté de faire ses achats dans des coopératives d'aliments complets biologiques et autres comportements de consommation écologique – ont démontré qu'il s'agit là de marchés spécialisés classiques. Autrement dit, un petit nombre de personnes exprimant des préférences très nettes peut soutenir un petit marché composé de nombreuses petites entreprises, mais les possibilités de croissance de ces marchés sont limitées, car même si d'autres consommateurs sont susceptibles de s'intéresser à une partie de ces produits, l'écart de prix mettra ceux-ci hors de leur portée, ou encore les coûts de transaction, en temps et en effort, seront trop élevés[15]. A moins que ces produits n'offrent vraiment au consommateur une valeur optimale, à moins également que les préférences environnementales ne soient très affirmées, la demande sera limitée, et même des incitations modestes par les prix n'auront que des effets marginaux[16]. C'est seulement à l'occasion que la demande de ce type de produits peut être stimulée par un marketing énergique, lorsqu'une grande entreprise à la

14. Pour un examen des facteurs qui justifient l'adhésion et qui montrent que celle-ci ne traduit pas simplement un calcul économique, voir Weick K.E., 1995, *Sensemaking in organisations*, Sage, Londres et Weick K.E., 2001, *Making sense of the organisation*, Blackwell, Oxford.

15. Sur les coûts élevés de transaction, en temps et en effort, qui ont freiner la volonté, par exemple, d'adopter le compostage domestique, voir Åberg H., Dahlman S., Shanahan H., et Säljö R., 1996, « Towards sound environmental behaviour: exploring household participation in waste management », *Journal of consumer policy*, 19, 1, pp. 45-67.

16. Bech-Larsen T., 1996, « Danish consumer's attitudes to functional and environmental characteristics of food packaging », *Journal of consumer policy*, 19, 3, pp. 339-363; Thøgerson J., 1999, « The ethical consumer: moral norms and packaging choice », *Journal of consumer policy*, 22, 4, pp. 439-460; Thøgerson J., 1994, « Monetary incentives and environmental concern: effects of a differentiated garbage fee », *Journal of consumer policy*, 17, 4, pp. 407-442.

marque solidement reconnue est prête à adopter ces produits pour internaliser les coûts. Les chaînes de supermarchés du Royaume-Uni et d'Europe continentale ont ainsi fait augmenter la demande d'aliments exempts d'OGM et biologiques, tout au moins pour un temps, mais elles ont malgré tout éprouvé des difficultés à la soutenir, et les ménages à faible revenu continuent de trouver ces produits inabordables. Les études sur les campagnes positives (*« buycotts »*), qui sont menées par les consommateurs qui expriment des préférences très arrêtées en faveur de l'achat exclusif de biens et services dont les fournisseurs ont internalisé certains coûts pour offrir les caractéristiques désirées, même si cela suppose un surprix, donnent à penser que ces stratégies sont peu fréquentes[17], qu'elles parviennent rarement à susciter une réaction favorable du côté de l'offre à une échelle véritablement importante sans bénéficier du puissant soutien de facteurs fondés sur la crainte, tels que l'action réglementaire visant à interdire les services de substitution[18], et qu'elles sont très difficiles à maintenir, surtout si la demande est essentiellement concentrée dans des créneaux spécialisés et qu'il y ait un écart de prix défavorable.

La question-clé qu'il convient alors de se poser au sujet des services à TPVP intégrée est de savoir si la demande de protection de la vie privée est comme la demande de produits écologiques, ou si elle exprime le besoin d'un bassin de consommation plus vaste, surtout lorsqu'il y a des écarts de prix défavorables entre les services qui utilisent les TPVP et les autres. J'examinerai plus attentivement les données disponibles dans la prochaine section, mais la plupart des études donnent à penser que les consommateurs exprimant des préférences très marquées en matière de protection de la vie privée et qui consentiront, pour les satisfaire, à payer un prix plus élevé pendant de longues périodes, constituent probablement une minorité dans la plupart des pays, mais que ces préférences gravitent davantage autour de certains biens et services que d'autres. En particulier, si autant de gens attribuent un degré de « sensibilité » unique aux données qui concernent leur état de santé et leur situation financière, le consentement à payer un surprix pour les services utilisant les TPVP sera peut-être plus répandu dans des secteurs comme les services financiers, les assurances et les soins médicaux que dans d'autres.

Tous ces exemples illustrent la difficulté qu'il y a à persuader les entreprises d'internaliser des coûts dont elles craignent que leurs concurrents puissent tirer un avantage à leur encontre en les externalisant, ainsi que l'équilibre entre espoir et crainte qui intervient dans le processus de persuasion. L'économiste d'entreprise S. Prakash Sethi, dans l'ouvrage qu'il a écrit avec Linda Sama[19], résume bien cette argumentation selon laquelle les facteurs intervenant dans la crainte et l'espoir (qui pourraient pousser les entreprises à internaliser des coûts dont elles pourraient craindre que leurs concurrents les externalisent) sont inégalement répartis dans l'économie. En effet, Sethi et Sama, dans leur étude des pressions exercées sur les entreprises pour qu'elles adoptent un comportement éthique, de façon générale, recensent un certain nombre de stratégies mises en œuvre par les régulateurs pour tenter de persuader les entreprises d'internaliser les coûts, qui peuvent se révéler judicieuses dans chacune de ces situations. La figure 1 ci-après constitue, je l'espère, un reflet ou une adaptation relativement fidèle de leur représentation graphique de cette analyse du problème, bien que les intitulés de certains des secteurs et l'équilibrage des facteurs d'espoir et de crainte soient

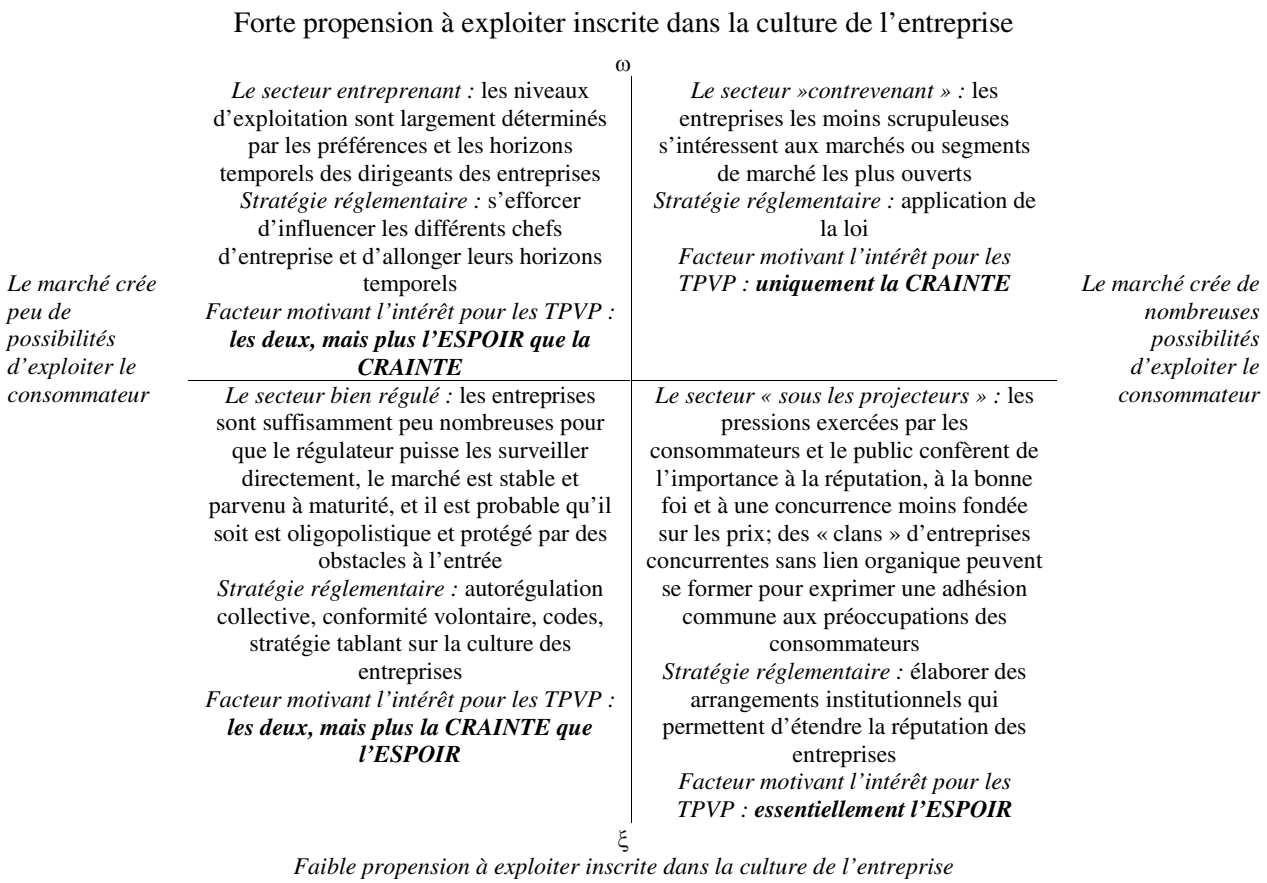
17. Friedman M., 1996, « A positive approach to organised consumer action: the "buycott" as an alternative to the boycott », *Journal of consumer policy*, 19, 4, pp. 439-451.

18. Neuner M., 2000, « Collective prototyping: a consumer policy strategy to encourage ecological marketing », *Journal of consumer policy*, 23, 2, pp. 153-175, notamment p. 172.

19. Sethi S.P. et Sama L.M., 1998, « Ethical behaviour as a strategic choice by larger corporations: the interactive effect of marketplace competition, industry structure and firm resources », *Business ethics quarterly*, 8, 1, pp. 85-104.

de moi[20]. Ces auteurs structurent la nature de ces différentes situations selon deux dimensions qui se croisent, décrivant la répartition des incitations. Ces deux dimensions sont le degré de militantisme des organes internes des entreprises contre l'exploitation du consommateur et le degré de création, par l'organisation du marché, des possibilités d'exploitation.

Figure 1. **La situation institutionnelle des entreprises détermine leur persuasibilité**



Source : D'après Sethi et Sama, 1998, p. 93.

20. J'ai apporté un changement de fond à l'analyse de Sethi et Sama. J'ai en effet réintitulé et modifié l'analyse du secteur décrit par le quadrant correspondant à un niveau de propension faible à exploiter mais avec de nombreuses possibilités d'exploiter. Même si j'ai suivi Sethi et Sama en déduisant, à partir des caractéristiques de situation, l'importance de la pression exercée par les consommateurs, de la réputation et de la bonne foi, je n'ai pas insisté comme eux sur certains autres facteurs. Ainsi, dans l'étude de Sethi et Sama, le quadrant est décrit comme un secteur « à forte croissance », associé à ce qu'ils appellent le stade moyen du cycle technologique et du cycle produit, avant que les innovations n'aient atteint les marchés de masse. Cependant, ces caractéristiques semblent fortement conditionnelles : dans de nombreux marchés spécialisés que décrit leur position structurelle de base, la forte croissance et le degré de préparation aux marchés de masse ne semblent pas être observés. J'ai tenté de centrer mon attention sur les caractéristiques qui découlent logiquement ou causalement de la position structurelle sur les deux dimensions.

Il sera important pour l'argumentation développée dans la prochaine section de voir que cette matrice peut être réagencée si l'on y introduit des dimensions légèrement différentes. Selon l'approche institutionnaliste des origines des préférences, l'importance des possibilités d'exploiter et celle de la propension à exploiter ne sont pas définies de façon totalement indépendante. En fait, la propension à exploiter et les préférences s'expriment et se précisent souvent en partie en fonction des possibilités perçues[21]. Les deux dimensions retenues par Sethi et Sama font apparaître en filigrane dans quelle mesure la surveillance exercée par la collectivité en général encadre à la fois la capacité et la volonté des entreprises d'exploiter, car c'est dans les secteurs où la surveillance est la plus faible, parce que son exercice est coûteux, que les entreprises les moins scrupuleuses évoluent et qu'elles trouvent les conditions propices à leur développement. Le fait d'avoir conscience d'être sous surveillance agit en effet comme une pression institutionnelle qui induit une volonté de restreindre l'exploitation et qui en limite donc les possibilités. Nous pouvons utilement introduire une dimension qui est implicite dans l'analyse de Sethi et de Sama, à savoir dans quelle mesure le marché est organisé selon une structure de monopole ou d'oligopole avec des barrières à l'entrée – ce qui crée quelque chose qui s'apparente à une autorité à l'intérieur du marché – et, inversement, dans quelle mesure il est ouvert à la concurrence, sans barrières à l'entrée. Cette mesure de la structure des marchés renseigne également sur la nature des modalités d'intervention de la surveillance. En effet, en situation d'oligopole, avec des barrières à l'entrée qui sont difficiles à franchir, le pouvoir direct du consommateur est atténué ; inversement, lorsque le marché est plus ouvert, ce pouvoir peut – selon l'autre variable qu'est la surveillance – avoir davantage de poids. En utilisant ces deux dimensions dans un tableau croisé, on peut produire exactement la même analyse des secteurs que Sethi et Sama. Cependant, ce réagencement de la matrice se révélera très important pour examiner la relation entre la différence de persuasibilité d'entreprises occupant des situations différentes et la différence de persuasibilité de consommateurs occupant des situations différentes, car il nous permettra d'obtenir une cartographie de la situation des entreprises qui sera exactement comparable à celle de la situation des consommateurs. Cette transposition de la classification des situations qui permet de dégager les différences de persuasibilité se traduit par la figure 2.

Quels types de TPVP les entreprises de chacun de ces secteurs de l'économie (qui font face à ces pressions structurelles émanant du marché, des consommateurs ainsi que du public en général et des régulateurs) sont-elles les plus susceptibles d'être persuadées d'utiliser ?

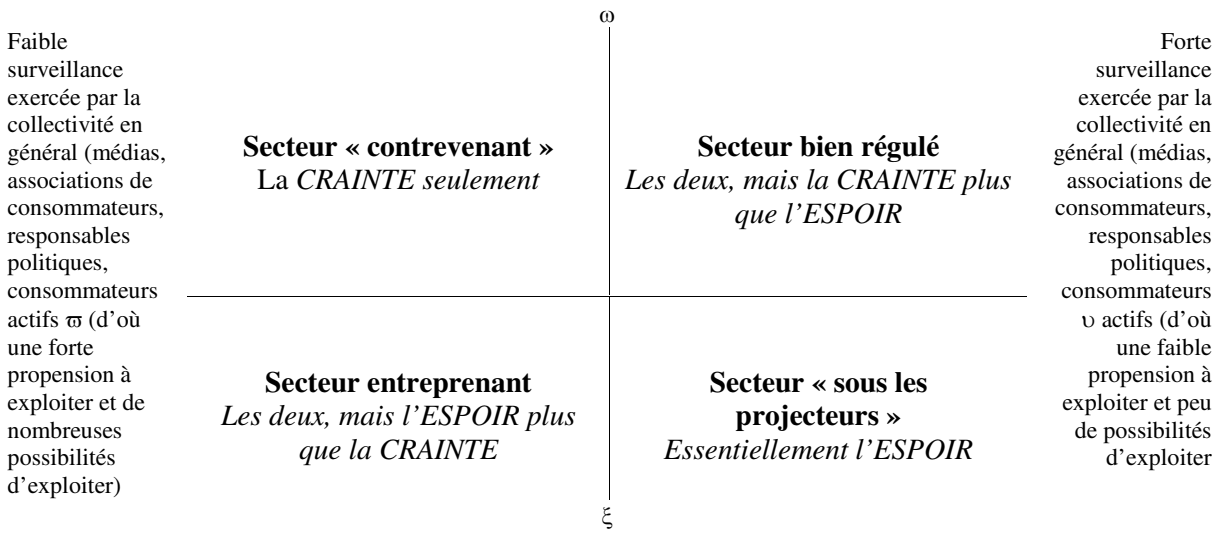
Pour répondre à cette question, nous avons besoin d'une classification des TPVP dans le sens général utilisé dans la présente étude et définie dans l'introduction. Il en existe certes de nombreuses en usage, mais pour notre propos, nous avons besoin d'une classification par fonction, c'est-à-dire par catégorie de risques contre lesquels la TPVP offre une protection – plutôt que par type technologique[22]. C'est en effet la fonction qui intéresse au premier chef les entreprises, même si le

21. Pour une étude institutionnaliste de la dynamique des marchés qui expliquent la production des préférences ainsi que la structure des possibilités dans le même processus, voir Douglas M., 1986, *How institutions think*, Routledge and Kegan Paul, Londres; Powell W.W. et DiMaggio P.J., (dir. publ.), 1991, *The new institutionalism in organisational analysis*, University of Chicago Press, Chicago; Thompson M., Ellis R. et Wildavsky A., 1990, *Cultural theory*, Westview Press, Boulder, Colorado; voir aussi Wildavsky A., 1994, « Why self-interest means less outside of a social context: cultural contributions to a theory of rational choices », *Journal of theoretical politics*, 6, 2, pp. 131-159, reproduit dans Wildavsky A., 1998, *Culture and social theory*, sous la direction de Chai S-K et Swedlow B, Transaction Publishers, New Brunswick, New Jersey, pp. 231-258. et en particulier 251 et suivantes.

22. La récente étude de l'OCDE offre, selon les termes utilisés ici, une classification technologique (paragraphe 2) ainsi qu'une classification fonctionnelle (paragraphe 12). Dans l'étude de l'OCDE, ce qui se rapproche le plus de la méthode actuelle axée sur le type de risque est appelée « *policy effect* »

coût sera bien sûr le deuxième élément à intervenir tout de suite après. La figure 3 illustre cette classification fonctionnelle.

Figure 2. **Transposition de la figure 1**



Source: Auteur.

L'étape suivante consiste à définir les implications relatives de chaque type de TPVP du point de vue des coûts. Ce qui importe ici, ce n'est pas le prix d'achat initial, mais les coûts économiques à long terme liés à l'exploitation d'un système de gestion des données soumis aux contraintes qu'impose un type de TPVP, et il s'agira d'examiner les implications de chaque type de TPVP pour le modèle commercial de base ainsi que du point de vue des coûts administratifs. On ne peut guère parler des différences de coûts à long terme prévus des technologies qui exécuteront ces tâches, étant donné qu'à moyen terme, ces coûts dépendent en partie du niveau de la demande. Ainsi, une demande plus forte fera en général augmenter les prix à court terme, mais dès lors que l'offre augmentera pour y répondre et que les coûts d'investissement seront récupérés, les prix baisseront en général entre le moyen et le long terme. Les coûts à long terme dépendent en partie de la taille du bassin de clientèle, de la valeur des services dans lesquels sont incorporés les TPVP, ainsi que de la longévité et de la valeur de la relation avec le consommateur. Cependant, il semble raisonnable de supposer qu'à court terme, ce sont les systèmes dans lesquels seront intervenues les modifications les plus importantes par rapport aux pratiques de gestion des données en vigueur qui représenteront vraisemblablement, au total, les coûts les plus élevés pour les entreprises. A long terme, l'intégrité de l'ensemble de données (c'est-à-dire son utilité pour couvrir la population que l'entreprise cherche à atteindre, ainsi que la cohérence des données détenues au sujet de chaque personne) détermine l'usage qui peut en être fait. C'est pourquoi, lorsque les TPVP ont une incidence sur ces éléments, on peut s'attendre qu'elles génèrent les coûts économiques véritables les plus importants (coûts d'opportunité), même si les coûts les plus importants enregistrés dans la comptabilité de trésorerie n'apparaissent pas ici.

(paragraphe 12): Groupe de travail sur la sécurité de l'information et de la vie privée, 2001, *Annexe 2: Une étude des technologies protectrices de la vie privée,* Direction de la science, de la technologie et de l'industrie, Organisation de coopération et de développement économiques, Paris.

Figure 3. **Classification fonctionnelle des types de technologies protectrices de la vie privée (TPVP)**

Les TPVP peuvent avoir l'une ou l'autre des fonctions suivantes :

1. *Notification*: permettre la notification de la collecte, de l'identité du maître du fichier, de la nature de l'utilisation, de la divulgation, etc.
2. *Consentement*: permettre l'expression du consentement ou du refus avant la collecte, par les moyens suivants :
   a. consentement explicite préalable (« *opt-in* »), ou
   b. mécanisme de refus explicite (« *opt-out* »)

   et ce :
   i. pour tout type de collecte de données.
   ii. pour la collecte de catégories définies (par ex, qui sont jugées particulièrement « sensibles »)
3. *Limitation du type de collecte:* limitation de la quantité ou du type d'informations collectées selon une certaine règle indépendante du consentement, et en général selon un certain codage qui est défini par l'objectif légitime.
4. *Limitation des contextes de collecte:* limitation des contextes dans lesquels de l'information peut être collectée ; ces contextes doivent correspondre à des descriptions précises (définis indépendamment du consentement et peut-être par l'objectif légitime).
5. *Accès de la personne concernée:* la technologie permet de donner à la personne concernée accès aux données collectées à son sujet.
6. *Possibilité de modifier les données:* la technologie permet à la personne concernée d'avoir accès aux données collectées à son sujet et de demander, le cas échéant :
   a. une correction ;
   b. la suppression d'informations jugées abusives ou non pertinentes ;
   c. la suppression complète du fichier la concernant.
7. *Alerte*: mise en place de « fils déclencheurs » dans l'utilisation de l'information, par exemple, instructions du type « arrêtez-vous et réfléchissez », « arrêtez-vous et vérifiez », avant l'utilisation de l'information :
   a. en vue de certaines finalités ;
   b. pour procéder à certains types d'inférence, par exemple pour des classifications dérivées qui pourraient être considérées comme constituant un délit.
8. *Limitation de l'identification:* limitation de la présentation de l'identification: c'est-à-dire de la possibilité d'identifier l'individu à partir de l'information accessible à des personnes non autorisées, par l'utilisation d'un pseudonyme et/ou en bloquant les autres informations clés recueillies.
9. *Limitation de la destination:* limitation, selon une règle, des possibilités de destination de divulgation, par exemple prévention de la copie des données.
10. *Information*: notification à la personne concernée des règles, codes et autres instruments acceptés par les maîtres de fichiers pour la collecte, la finalité, les usages effectifs et la divulgation, ainsi que de tout recours accessible, sur le plan interne ou auprès des autorités réglementaires.

Source: Auteur.

Sur cette base, les TPVP les moins chères à mettre en œuvre seront par conséquent celles qui alerteront le personnel (7), ou qui renseigneront les consommateurs (10). Celles-ci, en effet, n'impliquent aucune modification majeure de la structure standard des bases de données. La catégorie suivante pourrait comprendre les systèmes permettant aux personnes concernées d'avoir accès à l'information collectée à leur sujet (5), et ceux qui procèdent à la notification individuelle (1). Fournir un accès en ligne sécurisé en temps réel à la personne concernée est coûteux, mais lorsque de nombreux autres services sont fournis en ligne de toute façon, le coût marginal ne sera peut-être pas très important. Les systèmes qui limitent la présentation de l'identification (8) peuvent être coûteux à mettre en œuvre mais leur surcoût est négligeable s'ils sont intégrés à de nouveaux systèmes, et ils ne sont pas toujours particulièrement coûteux à exploiter par la suite, selon les parties que l'on voudra empêcher d'identifier l'information et les inconvénients que cela leur causera. Cependant, ces systèmes augmentent dans une large mesure la complexité de la configuration d'une base de données, ainsi que des règles qui s'appliquent à l'extraction et aux rapports que l'on peut en tirer. Les systèmes qui permettent d'adresser des demandes individuelles de modification de données (6) sont coûteux à exploiter, car ils supposent beaucoup de travail au niveau des fichiers individuels, une partie de ce travail ne pouvant être entièrement automatisée, bien que cela puisse réduire d'autres coûts liés à

l'inexactitude (même si l'accès en ligne sécurisé en temps réel de la personne concernée comprend l'affichage au niveau individuel, il ne permet pas d'autoriser un changement au niveau individuel). Les technologies les plus coûteuses sont celles qui pourraient compromettre la couverture de la base de données qu'une entreprise veut constituer – par exemple, les technologies qui prévoient le consentement (2), la limite de collecte (3) et (4) – et celles qui pourraient compromettre les relations commerciales envisagées – telles que la limitation de destination (9). La figure 4 résume ces regroupements hypothétiques très approximatifs. Il va sans dire que j'accepte leur caractère très approximatif et très provisoire. Cependant, une échelle plus fine, si on pouvait la mettre au point, pourrait servir de la même façon dans l'argument ci-après, sans remettre en cause le raisonnement développé dans l'étude.

Figure 4. **Tranches de coûts approximatives suggérées pour les TPVP**

Tranche	Type de TPVP
A: coût le plus bas	7: alerte, 10: information
B	5: accès de la personne concernée, 1: notification
C	8: limitation de la présentation d'identification
D	6: demande de modification des données
E: coût le plus élevé	2: consentement, 3, 4: limitation de la collecte, 9: limitation de la destination

Source: Auteur.

Dans une certaine mesure, la forte pression exercée par les préférences des consommateurs sur les entreprises des différents secteurs déterminera dans quelle mesure celles-ci pourront être persuadées d'investir dans différents types de TPVP. Nous nous y attarderons dans la prochaine section, mais il est raisonnable, à ce stade, de formuler les hypothèses suivantes :

1. *Secteur « contrevenant »*: nous ne nous intéressons ici qu'aux entreprises sans scrupules qui ne respectent pas la vie privée. De nombreuses entreprises fournissant des produits illégaux sont au contraire attentives aux préférences des consommateurs en ce qui concerne les produits et la protection de la vie privée. Les entreprises illégales fournissant des drogues illicites, elles aussi, sont très attentives à l'évolution des goûts en matière de drogues et respectent scrupuleusement la vie privée des consommateurs. Nous nous intéressons toutefois ici uniquement aux entreprises qui sont prêtes à utiliser pour le traitement des données à caractère personnel des méthodes qui sont illégales, de sorte que les préférences des consommateurs en matière de vie privée n'ont dans ce secteur guère d'impact. Il est bien sûr tout à fait possible que ces entreprises ne soient par ailleurs engagées dans aucune autre activité illégale.
2. *Le secteur bien régulé:* dans ce secteur, les préférences des consommateurs ont du poids, mais la stabilité et la nature oligopolistique du marché font que ces préférences sont souvent prises en compte de façon beaucoup plus sérieuses à la suite d'une action réglementaire (crainte) que directement (espoir).
3. *Le secteur entreprenant:* dans ce secteur, les entreprises sont suffisamment petites et mobiles pour être en mesure de se distinguer en fonction de leur compréhension de la segmentation de la population de consommateurs, de sorte que celles qui veulent répondre aux attentes des consommateurs exprimant des préférences très marquées en matière de protection de la vie privée trouveront les moyens de se positionner pour le faire savoir à ce segment du marché, et celles qui sont moins scrupuleuses rechercheront plutôt des créneaux ou elles peuvent servir des consommateurs moins préoccupés par

leur vie privée où dans lesquels les pratiques de traitement des données ne seront pas aussi transparentes pour les consommateurs.

4. *Secteur « sous les projecteurs »:* c'est dans ce secteur que les préférences des consommateurs en matière de protection de la vie privée seront vraisemblablement les plus affirmées et les plus puissamment amplifiées par les mouvements de défense des consommateurs et des droits de l'homme, lesquels influenceront l'attention qu'y apportent les régulateurs. Les entreprises qui formeront des « clans » sans structure fixe[23] – en utilisant par exemple des labels de confiance (tels que BBB Online, Truste™ et Trust UK) – pour faire connaître l'importance qu'elles attachent collectivement aux questions de respect de la vie privée enverront aux consommateurs d'importants signaux et qui renforceront leur exposition aux préférences des consommateurs en matière de protection de la vie privée.

Les associations professionnelles peuvent être des forces qui agissent en faveur du respect des normes de protection de la vie privée et de l'utilisation des TPVP, parfois presque en qualité de régulateur, parfois dans le cadre de « clans ». Dans l'une ou l'autre de ces situations, toutefois, c'est dans le secteur bien régulé et le secteur « sous les projecteurs » que leur capacité d'attirer des membres sera la plus grande. Idéalement, on pourrait souhaiter que ces associations soient surtout efficaces dans les secteurs des petites et moyennes entreprises – qui seraient réparties entre le secteur entreprenant et le secteur « sous les projecteurs » – car ce sont ces entreprises qui ont en général le moins de ressources à consacrer à la recherche, à l'évaluation, à l'adoption et à l'apprentissage de l'utilisation des TPVP. Cependant, la capacité de ces associations à attirer des membres du secteur entreprenant est en général plus faible, car c'est dans ce secteur que la pression concurrentielle de la crainte que les concurrents n'externalisent les coûts est la plus forte.

Compte tenu des diverses fonctions que les TPVP peuvent remplir, ainsi que des tranches de coûts proposées et des différentes pressions auxquelles les entreprises des quatre secteurs sont exposées, nous pouvons formuler l'hypothèse ci-après en ce qui concerne les secteurs dans lesquels se trouveront les entreprises les plus susceptibles et les moins susceptibles d'être persuadées à l'égard de chaque type de TPVP. Toute la question est de savoir jusqu'où, dans la hiérarchie des tranches de coûts des TPVP, les entreprises dans chaque situation pourraient être prêtes à descendre. La figure 5 illustre l'hypothèse qui se dégage de l'application du cadre défini dans la figure 2 aux tranches de coûts proposées dans la figure 4.

Si l'on accepte le raisonnement développé jusqu'ici, quelle stratégie les régulateurs chargés de la protection des données, les ministères chargés de surveiller les pratiques du monde des affaires en matière de gestion de données, et les mouvements de consommateurs et de défense des droits de l'homme préoccupés par la protection de la vie privée dans le secteur commercial ainsi que les organismes d'autorégulation comprenant des associations professionnelles mais également des organismes qui attribuent des labels de confidentialité, devraient-ils suivre pour persuader les entreprises d'investir dans les TPVP ?

23. Ouchi W.G., 1980, « Market, bureaucracies and clans », *Administrative sciences quarterly*, 25, 2, pp.120-142.

Figure 5. **Persuasibilité relative à l'égard des investissements dans les types de TPVP, par secteur**

Marché monopolistique/oligopolistique, barrières importantes à l'entrée

Faible surveillance exercée par l'ensemble de la collectivité (d'où une forte propension ϖ à exploiter et de nombreuses possibilités d'exploiter)	**Secteur « contrevenant »** Aucune	**Secteur bien régulé** *persuasibilité la plus grande:* alerte, information *persuasibilité moyenne;* accès de la personne concernée, limitation de l'identification, demande de modification de données *persuasibilité la plus faible:* consentement, limitation de la collecte, limitation de la destination	Surveillance vigilante exercée par la υ collectivité en général (d'où une faible propension à exploiter et peu de possibilités d'exploiter)
	Secteur entreprenant *(certaines entreprises seulement)* *persuasibilité la plus grande:* alerte, information, accès de la personne concernée *persuasibilité moyenne:* limitation de l'identification, demande de modification des données *persuasibilité la plus faible:* consentement aux demandes de modification de données, limitation de la collecte, limitation des destinations	**Secteur sous les projecteurs** *persuasibilité la plus grande:* alerte, information, accès de la personne concernée, limitation de l'identification, demande de modification de données *persuasibilité moyenne:* consentement, limitation de la collecte, limitation de la destination *persuasibilité la plus faible:* aucune	

ξ

Marché concurrentiel, faibles barrières à l'entrée

Note: Dans cette figure, on entend par « persuasibilité la plus forte/persuasibilité moyenne/persuasibilité la plus faible » le « degré de sensibilité à la persuasion visant à faire investir les entreprises dans les types de TPVP indiqués par rapport aux *autres types de TPVP*. Je suppose que les tranches de coûts des différents types de TPVP établies à la figure 4 sont les mêmes pour les différents secteurs et que la structuration générale est par conséquent la même. Cependant, dans certains secteurs, la volonté d'internaliser les coûts des tranches de coûts les plus élevées des TPVP devrait être, pour cette raison, plus forte que dans d'autres secteurs.

Source: Auteur.

La première question stratégique consiste à déterminer s'il faut concentrer les rares ressources disponibles pour la persuasion sur les entreprises qui sont les plus faciles à persuader – et qui sont bien sûr les moins susceptibles en général d'exploiter les consommateurs – ou au contraire sur celles qui sont les moins persuasibles. En théorie, il s'agit là d'un choix difficile du point de vue de la politique sociale, car il exige que l'on concilie urgence et faisabilité, mais en pratique, les organismes publics décident invariablement d'emprunter la première voie et c'est la faisabilité qui l'emporte chaque fois. Politiquement, étant donné l'obligation impérieuse de réaliser des « gains rapides », la nécessité de constituer des compétences en matière de persuasion et des capacités de collecte d'informations auprès de ceux que l'on persuade, et le fait que dans un pays développé capitaliste régi par les principes de l'État de droit, de nombreuses entreprises sont relativement persuasibles, il n'existe guère d'autre choix que de se concentrer sur celles qui sont les plus faciles à persuader, même si les risques les plus graves sont liés à celles qui sont les plus difficiles à persuader. C'est semble-t-il sur cette hypothèse qu'est fondé le conseil général adressé par Sethi et Sama aux régulateurs (voir figure 1).

Comme le notent Sethi et Sama, s'agissant du secteur « contrevenant », la seule force véritablement persuasive est celle de l'application des lois. On se trouve là dans un espace où l'espoir n'a guère de poids et où la crainte est le seul outil de persuasion à la disposition des organismes publics.

Les programmes de formation systématique à l'intention des entreprises dans le domaine de la protection de la vie privée ont connu un développement considérable : les cabinets de juristes, les bureaux de consultants en management, les groupes attribuant les labels de confiance, les réseaux professionnels de hauts responsables de la protection de la vie privée et les organismes consultatifs spécialisés en protection des données ont mis au point de tels programmes dans de nombreux pays. Les observations formulées ici sur la sensibilité à la persuasion tendraient à montrer que ces structures de formation institutionnalisée seront plus souvent utilisées dans le secteur *bien régulé,* où des parts de marché stable, des marchés et technologies parvenus à maturité ainsi que des systèmes hiérarchiques et bureaucratiques de gestion de données sont le plus souvent la norme. Deuxièmement, ces moyens de persuasion devraient attirer au moins un certain intérêt sur le secteur *sous les projecteurs,* où l'on ne s'attendra peut-être pas à trouver de responsables spécialisés en conformité, mais où il serait possible d'attirer, par une formation en bonne et due forme, divers types de personnel intervenant dans la gestion de données. Le plus grand intérêt que portent ces secteurs à ce type de soutien découle du fait qu'ils sont davantage exposés à la surveillance. Cependant, dans le secteur entreprenant, cette approche plutôt bureaucratique a beaucoup moins de chance d'être fructueuse. Si un intérêt pour ces programmes de formation se manifeste dans le secteur « contrevenant », ce sera en général dans les cabinets de juristes qui représentent les entreprises de ce secteur ou alors chez les gestionnaires intéressés uniquement à utiliser ce qu'ils auront appris dans ces cours pour trouver de meilleures façons de dissimuler leurs pratiques ciblées.

S'agissant des entreprises du secteur *entreprenant* et peut-être de certaines industries dominées par les petites entreprises dans le secteur *sous les projecteurs,* des techniques beaucoup plus informelles de diffusion de l'information à des fins de persuasion seront sans doute plus efficaces qu'une formation systématique. Dans le secteur entreprenant, il y a lieu de croire que des structures plus souples et moins individualistes telles que les réseaux de relations, seront plus indiquées. Elles pourraient aussi revêtir un certain intérêt dans certaines parties du secteur *sous les projecteurs*, mais il sera probablement plus efficace d'agir dans le cadre de structures de type « clanique » pour dégager une adhésion aux TPVP dans le cadre des « critères d'admission » aux clubs de labels de confiance et autres organismes ayant vocation à renforcer la réputation et à faire connaître les pratiques des entreprises aux consommateurs.

Il serait peut-être possible d'introduire les TPVP furtivement, comme cela s'est déjà fait, en commercialisant une technologie et un outil auprès des entreprises uniquement sur la base de leur fonctionnalité pour le traitement de données, de façon à éviter que les entreprises s'inquiètent des implications, sur le plan des coûts, des mesures en faveur de la protection de la vie privée des consommateurs, en leur laissant entendre qu'il s'agit seulement des coûts de fonctionnement normaux liés au traitement des données concernant les consommateurs. Pour ce faire, il faut incorporer les TPVP dans divers produits sans nécessairement attirer l'attention sur les aspects qui concernent la protection de la vie privée. Dans ces stratégies, on cherche à faire l'économie de l'étape de la persuasion afin de passer directement, espère-t-on, à celle où le produit s'impose de façon définitive, ou tout au moins à celle de l'habitude. Comme je l'ai fait remarquer plus haut, il est peu probable que ces techniques de manipulation soient opérantes pendant très longtemps. Cependant, la situation est très différente quand il s'agit de la création de normes convenues sur les produits et procédés dans le cadre des organismes nationaux, européens et internationaux chargés de veiller à l'application des meilleures pratiques en matière de protection de la confidentialité des données, y compris l'utilisation des TPVP, dans les procédés de gestion, d'organisation et d'exploitation. Le sujet a été amplement débattu au niveau européen, mais il semble avoir été mis de côté, tout au moins pour le moment, en raison de l'opposition des entreprises[24]. Cependant, l'Association canadienne de normalisation a

24. Le Comité européen de normalisation (CEN) a publié une première version d'un document de consultation précisément sur cette question. Cependant, dans sa version révisée, il a recommandé en

adopté une telle norme en 1996 – (au Canada, contrairement à ce qui se passe dans les autres pays, il semble que les groupes de défense des intérêts des petites entreprises soient parfois prêts à adhérer à une réglementation qui ne bénéficierait pas du même soutien dans d'autres pays, lorsqu'elles jugent que cela peut contribuer à instaurer des règles plus égales entre les petites et les grandes entreprises). Cependant, les décisions des premières entreprises qui adoptent une norme proposée traduisent un effet de persuasion : c'est seulement quand il ne reste que les derniers traînards sur la courbe en S conventionnelle que les économistes utilisent pour modéliser les rythmes d'adoption des innovations[25], que l'on peut s'en remettre à l' « impossibilité de faire autrement » pour garantir l'adoption, sans avoir recours à la persuasion. L'élaboration de normes relatives aux TPVP est un processus qui doit être vu non pas comme une stratégie de persuasion en soi pour les régulateurs mais comme un moyen d'appuyer les stratégies commerciales très différentes fondées sur l'espoir des entreprises situées dans chacun des trois secteurs autres que le secteur « contrevenant ».

Ainsi, se termine la section consacrée à la persuasibilité des entreprises à l'égard de l'internalisation des coûts des TPVP dont elles pourraient craindre que leurs concurrents les externalisent, aux types de TPVP à l'égard desquelles chaque secteur est, d'un point de vue structurel, le plus « persuasible » et les moyens par lesquels la persuasion peut le plus efficacement être exercée dans chaque secteur. La prochaine section examinera les variations de situations des consommateurs afin de voir comment consommateurs et entreprises dans différentes situations se comportent les uns avec les autres.

Persuader les consommateurs

Il a été avancé plus haut que pour déterminer quels consommateurs réclameront les types de protection de la vie privée que peuvent offrir les technologies incorporées, il nous fallait comprendre les différences entre les consommateurs à l'égard des éléments suivants :

- *Perception des risques :* différences entre les perceptions des risques d'atteinte à la vie privée, et possibilités d'influencer ces perceptions.
- *Sensibilité aux prix :* comment s'effectue l'arbitrage entre d'une part les préférences en matière de protection de la vie privée et d'autre part les écarts de prix entre les services qui utilisent les TPVP et ceux qui ne les utilisent pas.
- *Coûts de transactions :* comment les consommateurs se distinguent dans leur consentement à assumer les coûts de transaction parfois non monétaires de la recherche de fournisseurs et de la mobilité entre fournisseurs, et en ce qui concerne le temps et l'effort personnels qu'ils doivent consacrer à l'utilisation des mécanismes de protection qui leur sont offerts (par exemple, vont-ils effectivement faire valoir leurs droits d'accès de la personne concernée ou demander des corrections ?), et comment la situation peut varier selon qu'une concurrence plus ou moins forte s'exerce sur le marché.

---

définitive de ne pas élaborer de normes de gestion, mais de suivre l'évolution de la situation dans le cadre des organismes internationaux de normalisation et d'autres instances, de mener de travaux que sur les modalités des contrats ainsi que sur les critères d'attribution des labels de confiance aux entreprises qui respectent la vie privée des consommateurs, et de produire un autre rapport sur les TPVP : voir Comité européen de normalisation, 2001, « Initiative on privacy standardisation in Europe (IPSE) »: Document de travail – rapport du Groupe de projet pour le deuxième système de normalisation sur la société de l'information (ISSS), Atelier ouvert sur la confidentialité des données, Paris, 27 septembre 2001, CEN, Bruxelles, accessible sur: www.cenorm.be/isss.

25. Voir par exemple Gomulka S., 1990, *The theory of technological change and economic growth*, Routledge, Londres, ch. 6, et en particulier p.93.

Dans une autre étude, j'ai passé en revue les recherches consacrées à la perception du risque d'atteinte à la vie privée[26], pour faire valoir que la segmentation conventionnelle de la population en un petit groupe de « personnes non concernées », un groupuscule d'« intégristes » de la protection de la vie privée et un grand groupe de « pragmatiques » de la protection de la vie privée donne une image très déformée de la réalité[27]. D'abord, les perceptions des risques varient selon le contexte[28] : elles ne peuvent pas être cernées par l'application à la vie privée de types psychologiques sous-jacents stables. Ensuite, la catégorie des « pragmatiques » est trop vague et trop spacieuse pour être utile (de nombreuses enquêtes où elle est utilisée parviennent à la conclusion qu'entre les deux tiers et les trois quarts de la population en font partie !), et tend à favoriser dans les entreprises un optimisme exagéré qui leur faire croire qu'elles peuvent toujours offrir suffisamment de protection aux consommateurs, au point que ceux-ci cesseront un jour de se préoccuper des questions de vie privée. Autre problème également, cette classification ne présente pas de relations avec l'attitude dont nous estimons que les gens font preuve au sujet d'autres risques ou d'autres relations et pratiques en matière de consommation. Il serait en effet très étrange que la population pense et se situe différemment en ce qui concerne les préoccupations relatives à la vie privée et pratiquement toutes les autres préoccupations. Cette classification est également très statique. Elle ne permet pas de réfléchir à la façon dont les réactions des gens sont susceptibles de changer en fonction de l'évolution de leurs relations avec les entreprises et les administrations. Enfin, et c'est là une grave lacune de la classification « personnes non concernées – pragmatiques – intégristes », on ne sait pas d'où sont tirées ces catégories, ni exactement pourquoi quelqu'un aurait ce genre d'attitude à l'égard des questions concernant sa vie privée. Dire que « ces attitudes sont profondément ancrées dans les mentalités » ne constitue pas une explication, et encore moins une indication d'une quelconque utilité pour les régulateurs ou les entreprises qui veulent comprendre qui pourrait être sensible à quel type de persuasion, au sujet de quel type de risques, possibilités et mesures de protection.

Si nous cherchons une méthode qui prenne en compte le fait que la situation varie en fonction du contexte (même si certaines variations sont beaucoup plus difficiles à cerner que d'autres), qui soit plus précise, qui n'encourage pas un sentiment d'autosatisfaction trompeur, qui tienne compte du dynamisme, qui s'appuie sur une certaine explication de la perception des risques et qui soit mieux intégrée à ce qui, selon notre compréhension, détermine le mode de pensée des gens au sujet d'autres préoccupations, il faut aller au-delà de la psychologie. En effet, même si la recherche en psychologie sur la perception des risques a beaucoup à nous apprendre sur la variété des biais que nous pouvons observer[29], elle a essentiellement rendu compte de ce que l'on prétend être des heuristiques types

---

26. 6 P., 1998, en collaboration avec Lasky K. et Fletcher A., 1998, *The future of privacy, vol. II: public trust in the use of private information*, Demos, Londres.

27. Equifax 1995, *The Harris-Equifax mid-decade consumer privacy* survey, Equifax, Atlanta, Géorgie; Henley Centre for Forecasting, 1995, *Dataculture: privacy, participation, and the need for transparency in the information age*, Henley Centre for Forecasting, Londres; Direct Marketing Association et Informix, 1997, *The new information trade*, Direct Marketing Association et Informix, Londres.

28. Voir Sniderman P., 1993, 'The new look in public opinion research', dans Finifter A.W., (dir. publ.), 1993, *Political science: the state of the discipline II*¸ American Political Science Association, Washington DC, pp. 219-245 notamment p. 233.

29. La tradition psychométrique a été une source fertile d'observations de la distribution des types de biais dans la perception des risques – pour résumer, elle a été utile pour décrire la variable dépendante. Pour une vue d'ensemble, voir Slovic P., 1992, « Perception of risk: reflections on the psychometric paradigm », dans Krimsky S. et Golding D., (dir. publ.), 1992, *Social theories of risk*, Praeger, Westport, Connecticut, pp.117-152; Slovic P., 2000, *The perception of risk*, Earthscan, Londres; Kahneman D., Slovic P. et Tversky A., (dir. publ.), 1982, *Judgment under uncertainty: heuristics and biases*, Cambridge University Press, Cambridge; Kahneman D. et Tversky A., 2000, *Choices, values*

plutôt que des façons d'envisager les différences et les distributions, et elle ne nous a guère renseignés sur les biais qui interviendront chez telle ou telle catégorie de personnes, ni dans quelles circonstances[30].

Il est plus logique de commencer par comprendre où et comment les gens se situent dans l'organisation sociale, afin d'expliquer la perception des risques[31]. Cependant, la diversité des types de situations sociales de base dans lesquelles une personne peut se trouver n'est pas infinie[32] et nous pouvons utiliser une classification de base des formes d'organisation sociale pour nous aider à comprendre comment apparaîtront et pourront être comprises les différences de perception des risques à l'égard, notamment, de la vie privée.

Il peut être utile de commencer par un certain nombre de définitions qui seront utilisées dans la présente section pour décrire les facteurs situationnels qui façonnent la perception des risques. Par « situation de base » ou « primaire » d'une personne, j'entends la position intrinsèque, à long terme, que cette personne occupe par rapport aux principales forces institutionnalisées de la société dans laquelle elle vit, telles que le marché du travail, le marché de l'habitation, les services publics, les principaux fournisseurs de biens et services, ses pairs – collègues, amis et connaissances -, les institutions fondamentales comme la religion, l'organisation de la famille et d'autres encore. Par « contextes », j'entends l'ensemble des champs spécifiques au sujet desquels un individu est susceptible de fournir des renseignements à caractère personnel le concernant, par exemple dans ses rapports avec les détaillants, sa banque, son médecin et l'administration. C'est la situation primaire qui, selon le raisonnement que je développe ici, est le facteur réellement important, car c'est elle qui façonne le sentiment d'identité de l'individu, sa mentalité générale, ses capacités et ses préférences, en créant à la fois des contraintes et des possibilités et en limitant sa responsabilité à l'égard des institutions et des autres. Cependant, cette situation primaire est elle-même plurielle, car elle sera différente selon les contextes. Par exemple, bon nombre d'entre nous ont, avec leur médecin, une relation institutionnelle largement différente de celle qu'ils entretiennent avec le supermarché où ils font leurs courses. Notre attitude à l'égard de la perception des risques d'atteinte à la vie privée ne sera pas du tout la même en ce qui concerne notre dossier médical et l'information que détiennent les commerçants à notre sujet. Par « situation secondaire », j'entends, à beaucoup plus court terme, le contexte des conversations et interactions particulières qu'une personne peut avoir avec d'autres, qui

---

and frames, Cambridge University Press, Cambridge. Cette approche a été développée dans les travaux récents sur « la cartographie mentale » ; voir Morgan G., Fischhoff B., Bostrom A. et Atman C.J., à paraître en 2001, *Risk communication: a mental models approach*, Cambridge University Press, Cambridge; Bostrom A., Fischhoff B. et Morgan G.M., 1992, « Characterising mental processes of hazardous processes: a methodology and an application to radon », *Journal of social issues*, 48, 4, pp. 85-100, reproduit dans Löfstedt R. et Frewer L., (dir. publ.), 1998, *The Earthscan reader in risk and modern society*, Earthscan, Londres, pp. 225-238; Jungermann H., Schütz H. et Thüring M., 1988, « Mental models in risk assessment: informing people about drugs », *Risk analysis*, 8, 1, pp. 147-155, reproduit dans Löfstedt R. et Frewer L., (dir. publ.), 1998, *The Earthscan reader in risk and modern society*, Earthscan, Londres, pp.213-224. Pour une approche légèrement différente, voir Renn O., « Three decades of risk research: accomplishments and new challenges », *Journal of risk research*, 1,1, pp. 49-71.

30. Pour une critique de ces lacunes et d'autres faiblesses, voir Douglas M., 1985, *Risk acceptability according to the social sciences*, Russell Sage Foundation, New York, et Routledge and Kegan Paul, Londres.

31. Il s'agit là d'un argument qui n'est guère contesté en anthropologie et en sociologie, où la sociologie de la connaissance l'a développé depuis Durkheim et Evans-Pritchard.

32. Contrairement aux post-modernistes, qui estiment que la variation est infinie et sans aucun point d'ancrage dans les réalités de la vie sociale.

sont susceptibles, délibérément ou non, de tenter de la persuader d'adopter à l'égard du risque d'atteinte à la vie privée une autre opinion que celle découlant normalement de sa situation primaire. J'estime que des facteurs psychologiques tels que les traits de personnalité sont en général façonnés par la situation primaire, modulés selon le contexte, plutôt que déterminés ou induits indépendamment par des biais intervenant dans la perception des risques.

La figure 6 présente une synthèse de l'approche la mieux développée pour comprendre la perception des risques en général dans les sciences sociales récentes. Elle fournit une classification des formes de situation primaire qui produisent une pluralité limitée de types de perception des risques. Cette classification est produite par une matrice à deux dimensions, lesquelles sont identifiées par des descriptions légèrement plus accessibles des deux dimensions autour desquelles les sciences sociales gravitent depuis leur naissance. En 1897, dans *Le suicide*, Durkheim a introduit deux concepts pour comprendre comment la situation d'une personne dans l'organisation sociale déterminait sa propension au suicide. Ce qu'il appelle « régulation sociale » correspond ici à l'axe vertical, et son concept d'« intégration au groupe social » correspond à l'axe horizontal[33]. Depuis, divers autres termes, tels que « grille » et « groupe », ont été employés par le théoricien qui a été le premier à présenter cette matrice[34]. L'utilisation du tableau croisé permet de dégager quatre types fondamentaux d'organisation sociale, qui pourront se présenter dans n'importe quelle société humaine. Les types fondamentaux réapparaissent en économie sous la forme de marchés (individualisme), hiérarchies et clans (enclaves)[35] et la catégorie « isolement » est largement reconnue en sociologie et en

33. Durkheim É, [1897], Le suicide, Presses universitaires de France, Paris.

34. Douglas M., 1970, *Natural symbols: explorations in cosmology*, Routledge, Londres; Douglas M., 1982 [1978], « Cultural bias », dans Douglas M., 1982, *In the active voice*, Routledge and Kegan Paul, Londres, pp.183-254. Pour l'application à la perception du risque, voir Douglas M., 1992, *Risk and blame: essays in cultural theory*, Routledge, Londres; Douglas M. et Wildavsky A., 1982, *Risk and culture: an essay on the selection of technological and environmental dangers*, University of California Press, Berkeley; Adams J., 1995, *Risk*, UCL Press, Londres; Thompson M., Ellis R.J., et Wildavsky A., 1990, *Cultural theory*, Westview Press, Boulder; Coyle D.J. et Ellis R.J., (dir. publ.), 1993, *Politics, policy and culture*, Westview press, Boulder, Colorado; Dake K. et Wildavsky A., 1993, 'Theories of risk perception: who fears what and why?', dans Burger E.J., jnr, (dir. publ.), 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Douglas M., 1990, 'Risk as a forensic resource', *Daedalus*, 119, 4, 1-16; Douglas M., 1997, 'The depoliticisation of risk', dans Ellis R.J. and Thompson M., (dir. publ.), 1997, *Culture matters: essays in honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, pp.121-132; Ellis R.J. et Thompson F., 1997, 'Seeing green: cultural biases and environmental preferences', dans Ellis R.J. et Thompson M., (dir. publ.), 1997, *Culture matters: essays in honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, pp.169-190; Gross J.L. et Rayner S., 1985, *Measuring culture: a paradigm for the analysis of social organisation*, Columbia University Press, New York; Thompson M., Grendstad G. et Selle P., (dir. publ.), 1999, *Cultural theory as political science*, Routledge, Londres, Rayner S., 1992, 'Cultural theory and risk analysis', dans Krimsky S. et Golding D., (dir. publ.) 1992, *Social theories of risk*, Praeger, Westport, Connecticut, pp. 83-116.

35. Ouchi W.G., 1980, 'Market, bureaucracies and clans', *Administrative sciences quarterly*, 25, 2, pp.120-142. Pour une série de documents sur ce triple concept, voir Thompson G., Frances J., Levačić R., et Mitchell J., (dir. publ.), 1991, *Markets, hierarchies and networks*, Sage, Londres. On trouvera les premiers textes théoriques importants de la science économique sur les marchés et les hiérarchies dans Coase R.H., 1937, 'The nature of the firm', *Econometrica*, 4, pp.386-405. Un texte important plus récent dans Williamson O.E., 1986, *The economic institutions of capitalism*, Free Press, New York. Voir également Pitelis C., 1991, *Market and non-market hierarchies: theory of institutional failure*, Blackwell, Oxford, et Miller G.J., 1992, *Managerial dilemmas: the political economy of hierarchy*, Cambridge University Press, Cambridge.

anthropologie[36]. La matrice présente essentiellement une série d'hypothèses dont la validité a été vérifiée dans des travaux de recherche très divers sur les relations entre les situations et les attitudes à l'égard du risque en général.

Ces quatre types de situation peuvent se retrouver également dans l'attitude des consommateurs à l'égard des risques d'atteinte à la vie privée. Dans une récente étude qualitative que j'ai réalisée pour le gouvernement britannique, j'ai présenté l'application ci-après de la classification pour expliquer la distribution observée des attitudes à l'égard de la vie privée en rapport avec les propositions de partage de données personnelles entre ministères et organismes publics, ainsi que les pratiques qui s'y rattachent, destinées à promouvoir une administration « intégrée » ou holistique (figure 7)[37]. Au cours de discussions avec des groupes témoins, il a été possible de distinguer, pour chacune des attitudes de base à l'égard des risques, des formes plus modérées et des formes plus extrêmes d'application de ces attitudes aux risques d'atteinte à la vie privée. Cette application des attitudes de base permet de dégager, sous un concept global, des « profils », ou des modes de pensée spécifiques à l'égard des risques d'atteinte à la vie privée[38]. La Figure 7 représente l'ensemble des huit profils disponibles, que l'on obtient en comptant les formes modérées et extrêmes correspondant à chacune des quatre positions de base établies dans la figure 6. Là encore, il convient de ne pas perdre de vue que de nombreuses personnes passeront d'une position à l'autre à mesure qu'elles changeront de contexte.

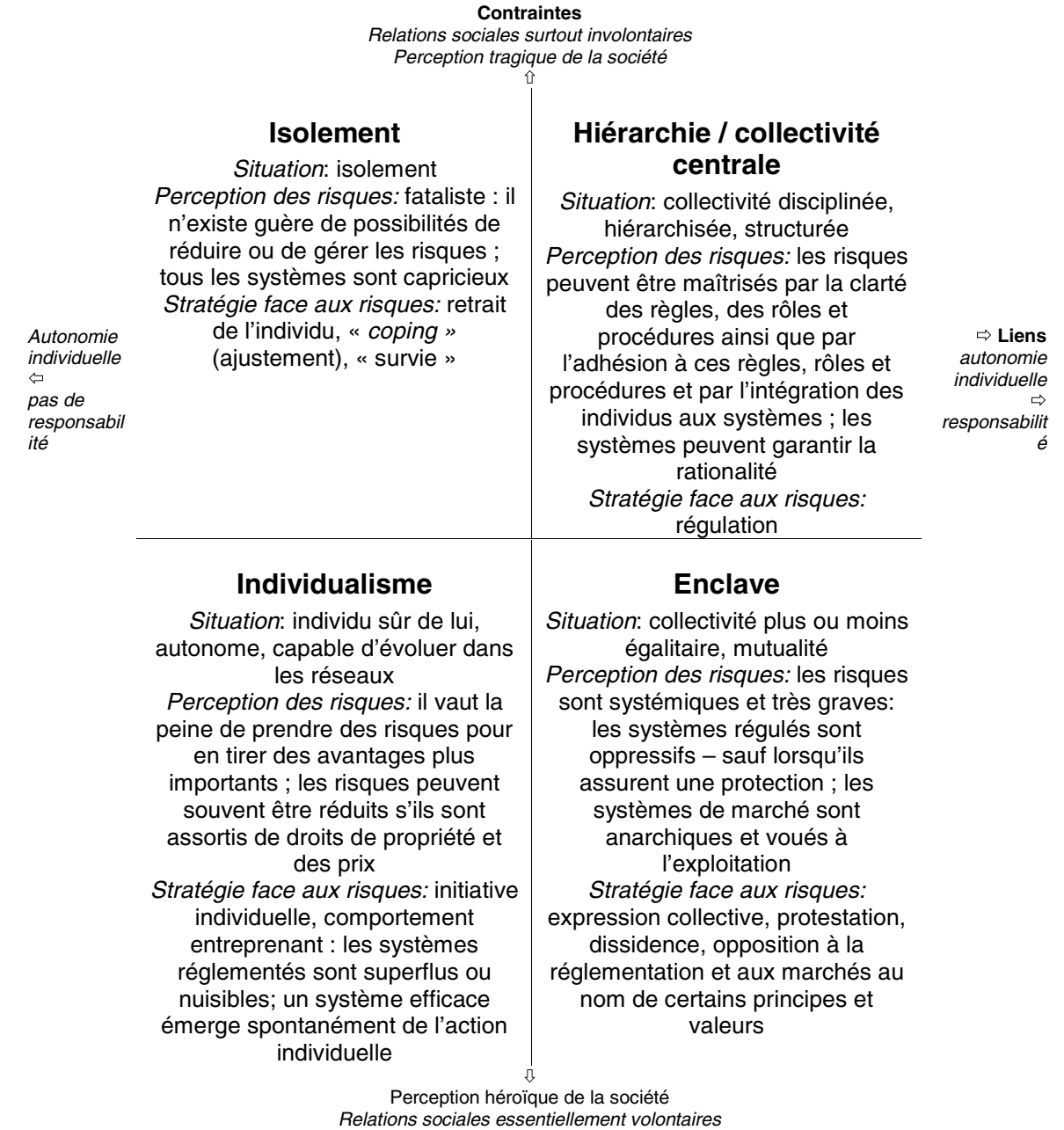
---

36. Dans l'analyse sociométrique des réseaux sociaux, on dispose de mesures structurelles bien développées de l'isolement : voir par exemple Wasserman S. et Faust K., 1994, *Social network analysis: methods and applications*, Cambridge University Press, Cambridge ; il existe aussi de nombreuses études qualitatives qui examinent les résultats associés aux positions d'isolement, en particulier les études sur l'adolescence : voir par exemple Cotterell J., 1996, *Social networks and social influences in adolescence*, Routledge, Londres. Les travaux sur le « capital social » ont mis en opposition les résultats associés aux formes d'isolement avec ceux associés aux autres formes. Voir Putnam R.D., 2000, *Bowling alone: the collapse and revival of American community*, Simon and Schuster, New York; Lin N, 2001, *Social capital: a theory of social structure and action*, Cambridge University Press, Cambridge. Dans les traditions de la sociologie et de l'analyse des réseaux sociaux, on trouve également un grand nombre d'études sur les enclaves – par exemple, Elias N., en collaboration avec Scotson J.L., 1994 [1977], *The established and the outsiders: a sociological enquiry into community problems*, Sage, Londres – et sur l'individualisme – en tout premier lieu celle de Granovetter, 1994 [1974], *Getting a job: a study of contacts and careers*, 2ème édition, University of Chicago Press, Chicago, et Burt R.S., 1992, *Structural holes: the social structure of competition*, Harvard University Press, Cambridge, Massachusetts. Pour un aperçu général, voir 6 P, 2001, 'The governance of friends and acquaintances? Public policy and social networks', communication présentée lors du séminaire conjoint du *Economic and Social Research Council* et de l'*Institute for Public Policy Research*, « Public policy and social networks: promoting social inclusion », 15 mars, Londres. Une étude classique de l'attitude fataliste à l'égard du risque, associée à des formes comparativement isolées, dans Banfield E.C., en collaboration avec Banfield L.F., 1958, *The moral basis of a backward society*, Free Press, New York.

37. Voir 6 P., 2001, *Strategies for reassurance: public concerns about privacy and data sharing in government*, Performance and Innovation Unit, Cabinet Office, Londres.

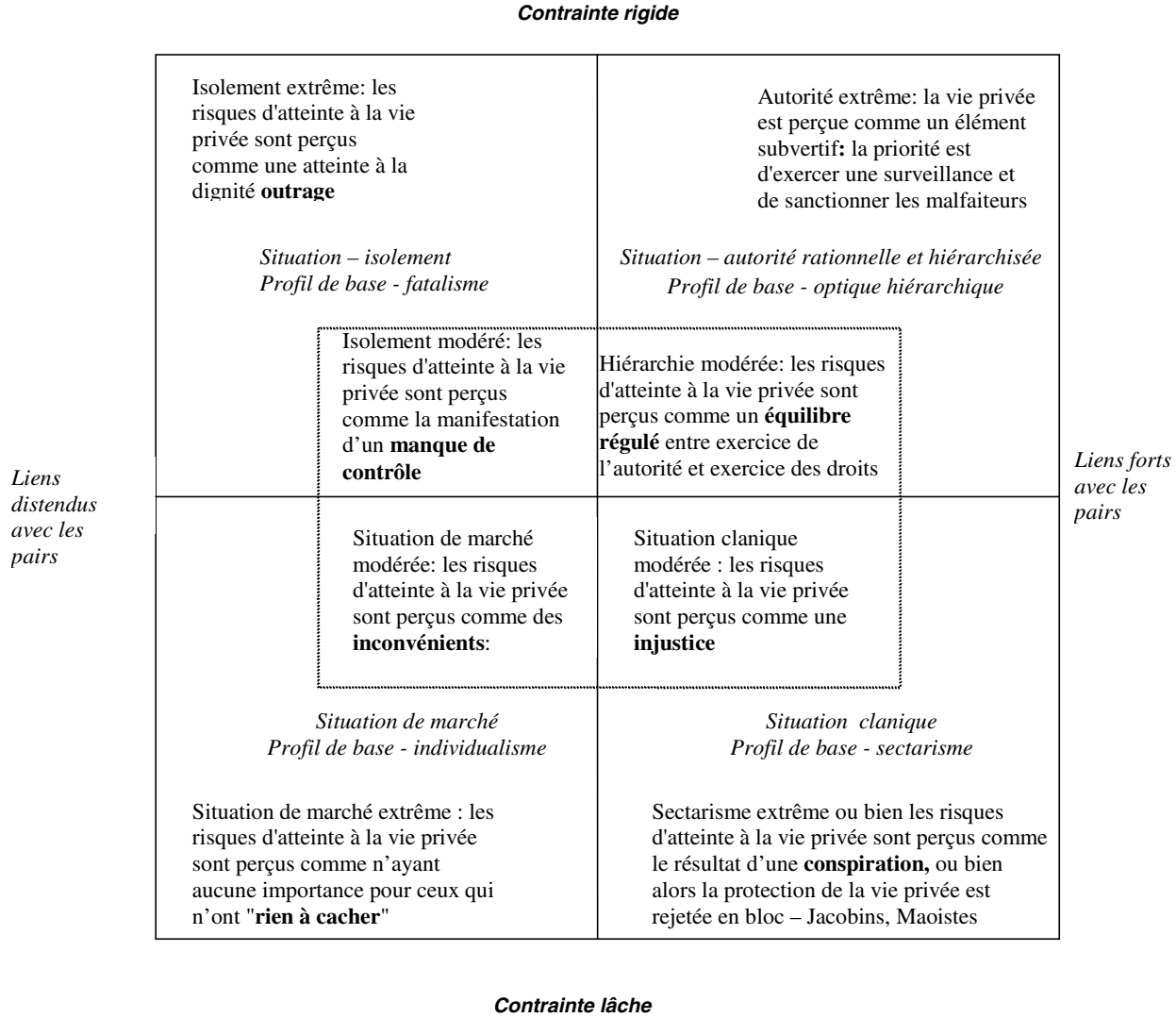
38. Gamson W.A., 1992, *Talking politics*, Cambridge University Press, Cambridge; pour un examen du concept de profil, voir 6 P., 2001, 'What's in frame? Social organisation, risk perception and the sociology of knowledge', manuscrit inédit, King's College, Londres.

Figure 6. **Comment la situation façonne la gamme fondamentale des perceptions d'un quelconque type de risque**



Source: Auteur.

Figure 7. **Comment la situation primaire détermine la façon dont les consommateurs perçoivent les risques d'atteinte à la vie privée**



Source: Auteur.

Dans l'étude mentionnée, les personnes les plus exclues de la société, qui étaient allocataires de prestations de longue durée, étaient en général isolées et correspondaient au profil « atteinte à la dignité », estimant que la collecte et le partage des données étaient humiliants et dégradants, mais aussi inévitables et faisant partie des mécanismes de la vie en société. En revanche, les travailleurs indépendants masculins qui agissaient en qualité d'intermédiaire dans des réseaux pouvaient se situer, au début, dans la catégorie « rien à cacher », étant d'avis qu'une personne n'ayant rien à cacher n'avait pas à se préoccuper de la protection de la vie privée, mais ils passaient rapidement à la catégorie « inconvénients », dans laquelle la collecte et le partage de données étaient considérés plus comme une nuisance que comme une menace. Certaines personnes âgées qui avaient grandi dans l'après-guerre et avaient fait l'expérience d'un engagement à l'égard de diverses institutions de solidarité dans des contextes tels que les soins de santé, mais qui avaient quitté le marché du travail et sa hiérarchisation particulière du statut social et avaient adopté une nouvelle identité – celle de retraité –, définie par des critères rigoureux, associaient les risques d'atteinte à la vie privée à des problèmes d'injustice, ou à la violation de principes généraux par l'État. Le profil le plus extrême – celui qui correspond à l'idée de

« conspiration » – est en général surtout associé aux mouvements de défense de la vie privée. Enfin, les membres les plus conservateurs des forces de l'ordre adhèrent au profil où l'on estime que la vie privée a un caractère subversif, soutenant avec insistance que sans une surveillance générale, il serait impossible de faire échec au crime et de le prévenir. En revanche, il est plus courant de voir les fonctionnaires de l'administration centrale, à qui il incombe de concilier au mieux les préoccupations des services chargés de l'application des lois et celles de divers autres publics plus larges, se situer dans le profil « équilibre régulé »[39], dans lequel on espère qu'il sera possible de définir un certain ordre quasi-constitutionnel et de le traduire dans des règles explicites qui réussiront à concilier les pressions conflictuelles de telle façon qu'il pourrait être administré par des moyens administratifs classiques[40].

Il n'est pas vraiment utile de procéder à des estimations quantitatives des proportions de la population qui pourraient être décrites par chacune de ces situations, précisément parce que la dynamique de ces situations est soumise, dans la vie de chacun, à une grande mobilité entre les contextes. Autrement dit, la situation primaire est en elle-même plurielle pour la plupart d'entre nous. Beaucoup se montreront en effet plutôt individualistes lorsqu'il s'agira de prendre une carte de fidélité dans un supermarché, avec toutes les divulgations d'informations personnelles que cela suppose au sujet de leurs habitudes de consommation, et adopter une attitude pourtant beaucoup plus enclavée dans la façon dont ils tiennent à ce que leur médecin gère l'utilisation et la divulgation de leur dossier médical, tout en étant satisfaits de croire qu'un certain dosage de surveillance réglementaire et de codes professionnels pourra régir adéquatement l'utilisation appropriée par leur banque des données concernant leurs transactions. Cette mobilité traduit la pluralité de nos relations institutionnelles avec les grandes sociétés de commerce de détail, les médecins et les banques, et nous renseigne sur les aspects contextuels plus larges de nos vies – éducation, religion, réseaux sociaux, classe, sexe, et ainsi de suite – qui interviennent dans chacun de ces contextes[41]. (Cela ne veut pas dire que les gens peuvent se déplacer à l'intérieur de cette matrice avec une égale facilité, ou qu'ils le font effectivement. Comme je le montrerai plus loin, la hauteur des obstacles à surmonter pour passer d'une position à l'autre varie considérablement). Bien que l'on ait tenté de produire des estimations d'un biais global de type « vision du monde », fondées sur des énoncés attitudinaux très généraux et indépendants du contexte présentés sous la forme d'une échelle de Likert (élaborée par le regretté Karl Dake) pour mesurer les positions individuelles à l'intérieur de la classification présentée à la figure 6[42], c'est

39. Pour une critique de l'argument selon lequel un « équilibre » peut devenir un critère aussi déterminé pour l'élaboration des politiques qu'on l'envisage dans cette structure hiérarchique bureaucratique, voir Raab C.D., 1999, 'From balancing to steering: new directions for data protection', dans Bennett C.J., et Grant R., (dir. publ.), 1999, *Visions of privacy: policy choices for the digital age*, University Toronto Press, Toronto, pp.68-93.

40. 6 P., 2001, *Strategies for reassurance: public concerns about privacy and data sharing in government*, Performance and Innovation Unit, Cabinet Office, Londres Pour une version antérieure qui situe bon nombre des principaux auteurs et penseurs qui se sont intéressés à la vie privée dans ces deux dimensions, voir 6 P., 1998, *The future of privacy, vol I: private life and public policy*, Demos, Londres, ch.4.

41. En ce qui concerne l'hypothèse de la « mobilité », voir Rayner S., 1992, 'Cultural theory and risk analysis', dans Krimsky S. and Golding D., (dir. publ.), 1992, *Social theories of risk*, Praeger, Westport, Connecticut, pp. 83-116.

42. Voir par exemple Grendstad G. et Selle P., 1997, 'Cultural theory, postmaterialism and environmental attitudes', dans Ellis R.J. et Thompson M., (dir. publ.), 1997, *Culture matters: essays in honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, pp. 151-168; Dake K. et Wildavsky A., 1993, 'Theories of risk perception: who fears what and why?', dans Burger E.J., jnr, (dir. publ.), 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Grendstad G., 2001, 'Nordic cultural baselines:

précisément parce que ces énoncés sont si généraux et indépendants des contextes qu'il y a lieu de mettre en doute leur utilité, à plus forte raison pour tenter de procéder à des comparaisons internationales.

Il pourrait être plus utile de disposer de données comparables au plan international sur les différences de perception par le public de divers types de risques d'atteinte à la vie privée dans des contextes précis. Mais il serait encore plus utile de mener des études comparatives internationales sur les variations des perceptions des risques d'atteinte à la vie privée selon le contexte et selon les différences de situation primaire. Pour cela, les techniques d'enquête de Dake et de ses successeurs n'auront d'utilité que si elles peuvent être mises en exacte corrélation avec des informations sur la situation primaire des populations étudiées. Certaines méthodes ont été élaborées à cette fin[43], mais elles n'ont encore fait l'objet d'aucune tentative d'application.

Étant donné que la perception des risques d'atteinte à la vie privée est un élément déterminant de l'intérêt porté aux TPVP, il y a lieu de penser, toutes choses étant égales par ailleurs, que les types de TPVP qui susciteront le plus d'intérêt, le cas échéant, varieront beaucoup selon ces différentes situations. Ainsi, les personnes les plus fatalistes n'accorderont probablement guère foi ni à l'efficacité, ni à la pertinence de la plupart des TPVP dans leur vie. Après avoir été pendant longtemps à la merci de grandes structures bureaucratiques en ce qui concerne l'information, les allocataires de prestations pensaient en général, dans l'étude où cette analyse a été affinée, qu'ils n'avaient guère la possibilité d'influencer, et encore moins de contrôler, par quelque moyen technologique que ce soit, l'usage que ces structures font de l'information personnelle les concernant. Les plus cyniques allaient même jusqu'à douter de pouvoir consulter leur dossier en ligne et à prétendre que l'information qui leur serait rendue accessible au nom du principe de l'accès de la personne concernée ne serait en fait pas le véritable dossier. Les attitudes « plus modérées » qui voient dans les risques d'atteinte à la vie privée un « manque de contrôle » pouvaient être associées, au minimum, à une propension à s'intéresser à l'accès en ligne de la personne concernée aux informations détenues à son sujet. Les personnes qui entraient dans la catégorie individualiste plus modérée (les risques perçus comme « inconvénients ») s'intéressaient en général, comme on pouvait le prévoir, aux instruments susceptibles de donner un accès plus individuel à l'information, notamment aux mécanismes de consentement faisant le moins obstacle aux avantages découlant de l'échange d'informations – par exemple les systèmes de refus explicite plutôt que les systèmes de consentement explicite. Pour cette catégorie, l'information sur les usages qui sont faits de leurs données est de la plus haute importance. En revanche, les personnes qui entrent dans la catégorie plus enclavée (les risques d'atteinte à la vie privée perçus comme « injustice »), et qui ont certainement une attitude davantage apparentée aux mouvements sociaux radicaux seront beaucoup plus enclins à s'intéresser aux technologies qui limitent la collecte de données ou qui permettent d'assurer l'anonymat ou le pseudonymat. De fait, l'ampleur de la collecte des données et l'absence d'anonymat en soi font partie des principales préoccupations des mouvements sociaux voués à l'organisation de la protection de la vie privée[44]. Enfin, les consommateurs qui adhèrent à une vision plus hiérarchique feront davantage confiance aux programmes et justifications des grandes organisations en tant que maîtres de fichiers, rechercheront essentiellement les TPVP qui leur permettent de corriger des erreurs mineures, et seront tout au plus disposés à utiliser certains outils de pseudonymat dans les domaines où ils le jugent approprié compte

---

accounting for domestic convergence and foreign policy divergence', *Journal of comparative policy analysis, research and practice*, 3, pp. 5-29.

43. Voir Gross J.L. et Rayner S., 1985, *Measuring culture: a paradigm for the analysis of social organisation*, Columbia University Press, New York.

44. Voir par exemple Davies S., 1996, *Big brother: Britain's web of surveillance and the new technological order,* Pan, Londres.

tenu des normes en vigueur, plus pour se protéger contre des atteintes individuelles que contre des abus de grandes organisations réglementées, aux procédures desquelles ils font au moins confiance pour le moment. Pour ce groupe, l'existence d'une loi exprimant l'adhésion à une valeur sociale – par exemple, loi sur la protection des données – a un pouvoir symbolique qui renforce cette valeur[45]. La figure 8 résume ce à quoi on peut s'attendre.

Figure 8. **TPVP susceptibles d'intéresser le plus les consommateurs, selon leur perception des risques**

Contraintes ω

Fatalisme	***Hiérarchie***
? accès de la personne concernée	1. alerte, information 2. accès de la personne concernée, possibilité de modifier les données 3.? Limitation de l'identification
Individualisme	***Enclave***
1. accès de la personne concernée, possibilité de modifier les données 2. refus explicite (« *opt-out* ») 3. information	1. consentement explicite (« *opt-in* »), limitation du type de collecte, limitation du contexte de la collecte, limitation de l'identification, limitation de la destination, notification 2. accès de la personne concernée

Liens υ

Source: Auteur.

Si nous estimons que nous disposons là d'une grille raisonnable de l'éventail d'attitudes des consommateurs à l'égard des risques d'atteinte à la vie privée, nous pouvons nous pencher sur la question de savoir dans quelle mesure les populations correspondant à ces différentes perceptions initiales peuvent être persuadées de changer de profil ?

L'argument qui sous-tend cette analyse donne à penser que la persuasion est possible, mais que, s'agissant d'influencer les consommateurs pour qu'ils s'intéressent à d'autres TPVP que celles vers lesquelles les porterait leur biais initial, ses limites apparaissent clairement, comme il a été démontré dans la section précédente que la persuasibilité des entreprises comportait elle aussi des limites bien visibles. En effet, ce qui détermine véritablement la perception des risques, c'est la situation. Autrement dit, si l'on est dans l'impossibilité de modifier la situation réelle dans laquelle se trouvent les consommateurs, on ne saurait s'attendre que leur perception des risques change beaucoup.

Cela étant dit, les possibilités de passer d'un profil à l'autre sont limitées. Jusqu'ici, nous avons examiné l'influence dominante de ce que nous pourrions appeler la situation *primaire* – c'est-à-dire la position fondamentale, dans la durée, que les consommateurs occupent dans la société par rapport aux grandes organisations, aux marchés, au marché du travail, à leurs pairs, telle qu'elle est modulée par les cadres institutionnels propres aux contextes particuliers.

Certaines personnes sont très peu mobiles, et en ce qui les concerne, les méthodes d'enquête au sujet desquelles certaines réserves ont été émises plus haut peuvent conserver une certaine validité si

45. Sniderman P.M., Piazza T., Tetlock P.E. et Feld P.J., 1991, 'The American dilemma: the role of law as a persuasive symbol', dans Sniderman P.M., Brody R.A. et Tetlock P.E. (dir. publ.), *Reasoning and choice*, Cambridge University Press, New York.

elles peuvent isoler les personnes représentatives. En général, les personnes qui demeurent dans le même quadrant dans tous les contextes de leur vie se situent en général aux extrêmes de la matrice de la figure 7. En effet, c'est en général aux extrêmes qu'un ensemble unique de caractéristiques globales de la situation primaire influe sur tous les aspects de la vie d'un individu – par exemple, grande pauvreté, grande richesse, engagement à vie au service d'un mouvement ou d'une collectivité, domination d'une église ou omniprésence de l'activité professionnelle. Dans la plupart des sociétés développées, ces types de situations concernent probablement une minorité de la population et il y a donc lieu de penser que des proportions importantes de la population présenteront au moins une certaine mobilité entre les contextes, en général entre les positions plus modérées.

En revanche, s'agissant d'induire un changement d'attitude à partir de situations secondaires (conversations ou rencontres au cours desquelles est véhiculée une information susceptible d'être en opposition avec le mode de pensée engendré par la situation primaire, et modulée par le contexte), la persuasion pourra, au mieux, déclencher des déplacements entre quadrants adjacents, qui ne dureront – et encore – que si elle est exercée de façon soutenue.

Ces arguments peuvent être formalisés par les trois hypothèses ci-après relatives aux possibilités d'induire par la persuasion ces déplacements entre quadrants voisins :

A. Les déplacements d'un extrême à l'autre dans le sens diagonal rencontre des obstacles moins importants que les déplacements dans le sens vertical ou horizontal

L'une des raisons, par exemple, pour lesquels les intérêts des entreprises et ceux des services chargés de l'application des lois peuvent parfois concorder sur les questions de protection de la vie privée est qu'il existe une affinité entre les extrêmes le long de la diagonale positive. Selon certains chefs d'entreprise, « si vous n'avez rien à cacher, vous n'avez pas à vous préoccuper de la protection de la vie privée ». Il est clairement apparu dans l'étude examinée plus haut que c'est là une position prise typiquement pour affirmer son honnêteté et mettre les autres au défi de montrer qu'ils sont eux aussi irréprochables en se ralliant à cet avis. Autrement dit, cet argument sert à détourner les soupçons. Les agents des forces de l'ordre qui s'ont d'avis que beaucoup de gens, dont on ignore le nombre, ont effectivement quelque chose à cacher et que c'est précisément pour cette raison que la vie privée ne devrait pas être protégée peuvent par conséquent s'allier à ceux qui entrent dans le quadrant « rien à cacher », car les uns comme les autres sont surtout intéressés à faire le tri parmi des populations potentiellement suspectes. Inversement, le quadrant « conspiration » dans lequel entrent les militants de la protection de la vie privée et leur vision déterministe selon laquelle les technologies de l'information sont par définition oppressives est à rapprocher de l'opinion inscrite dans le quadrant « atteinte à la dignité » selon laquelle les grandes organisations exploitent forcément la population : en fait, l'affinité constatée traduit le rôle de ces quadrants extrêmes, où est mobilisée la suspicion[46]. Ces affinités rendent les déplacements d'un quadrant à l'autre, dans certains types de conversation, plus faciles que d'autres.

46. S'agissant de savoir combien il importe de comprendre la perception des risques comme procédant essentiellement de l'organisation de ce qu'il faut faire des processus sociaux d'attribution de la responsabilité, voir Douglas M, 1992, *Risk and blame: essays in cultural theory*, Routledge, Londres.

B. *Les déplacements diagonaux à l'intérieur des quadrants rencontrent moins d'obstacles lorsqu'ils se font vers l'extérieur que vers le centre, la situation primaire contribuant à affaiblir éventuellement l'ancrage au profil de référence.*

Si par exemple une personne se trouve dans une situation d'insécurité sur le marché du travail, elle passera beaucoup plus facilement, en ce qui concerne la protection de la vie privée vis-à-vis de son employeur et des organismes gouvernementaux, du profil « manque de contrôle » vers le profil « atteinte à la dignité » lorsqu'elles sera placée dans la situation secondaire d'une conversation avec des personnes dont le profil de référence sera celui de l'atteinte à la dignité. De même, la personne qui se trouve en situation d'insécurité dans sa collectivité de résidence et se sent surveillée peut facilement passer du profil « injustice » au profil « conspiration » si elle est en conversation avec quelqu'un qui est moins modérément enclavé qu'elle.

C. *Les déplacements verticaux et horizontaux entre les positions modérées sont plus faciles à réaliser que les déplacements entre l'élément modéré d'un quelconque quadrant et l'élément extrême d'un autre quadrant apparenté horizontalement ou verticalement (mais pas diagonalement pour un groupe dont le profil de base ou de référence est suffisamment solidement associé à une attitude modérée.*

Les groupes témoins sur lesquels portait l'étude dont il est question ici comprenaient des personnes qui se trouvaient dans des situations primaires assez différentes. En conversation les unes avec les autres, bon nombre d'entre elles ont pu passer relativement facilement entre, par exemple, le profil « manque de contrôle » et le profil « injustice », mais aucune du profil « indignité » au profil « inconvénient ». Cependant, certains allocataires du RMI ont pu, après avoir longuement discuté ensemble, à se déplacer occasionnellement le long de la diagonale pour entrer dans le profil « injustice ».

Par quels moyens les organismes de réglementation peuvent-ils modifier des situations primaires ou créer des situations secondaires dans lesquelles les consommateurs pourraient être incités à changer d'attitude ? Premièrement, les régulateurs n'ont pas le monopole de la communication relative au risque dans ce domaine, ni ne s'adressent à un auditoire captif. De nombreux organismes et sociétés commerciales diffusent des messages également. Deuxièmement, il importe de noter que tous les moyens de persuasion et de propagande dont disposent les organismes publics sont des instruments dont l'efficacité n'est pas acquise. Il n'est pas certain qu'un organisme gouvernemental utilisant un instrument donné susceptible d'induire un changement d'opinion au sujet de la protection de la vie privée parviendra à faire adopter, à l'égard des risques d'atteinte à la vie privée, le point de vue qu'il privilégie. En effet, une fois que les citoyens se sont dissociés de leur profil/quadrant d'origine, leur évolution n'est pas prédéterminée[47]. On parviendra plus facilement à orienter le citoyen vers l'attitude souhaitée en agissant sur la situation primaire plutôt qu'en se limitant à offrir de l'information pour influencer la situation secondaire.

Modifier les situations primaires de base des populations constitue l'objectif le plus ambitieux des responsables politiques, qui doivent pour cela mettre en œuvre un panachage complexe de mesures incitatives, de réglementations autoritaires, d'information et de persuasion qui dépassent très largement le cadre de la présente étude, car ces moyens sont en général mobilisés pour des raisons beaucoup plus générales que pour simplement influencer les préférences en matière de protection de la

47. Thompson M., 1992, 'The dynamics of cultural theory and their implications for the enterprise culture', dans Hargreaves Heap S. and Ross A., (dir. publ.), 1992, *Understanding the enterprise culture: themes in the work of Mary Douglas*, Edinburgh University Press, Edimbourg, pp.182-202.

vie privée[48]. Pour influer sur les situations secondaires, on a essentiellement recours aux instruments d'information – éducation, communication, persuasion – que ce soit par l'entremise d'organismes officiels tels que les écoles ou par des systèmes informels tels que les médias. Les recherches revêtent en général que les résultats de ces stratégies varient beaucoup selon les circonstances particulières[49]. Si ces stratégies peuvent être menées pendant de très longues périodes, en bénéficiant de l'adhésion sans réserve de toutes les institutions locales, auprès de groupes cibles définis, et si elles peuvent mises en œuvre avec une intensité telle que le pouvoir de l'information s'assimile en quelque sorte à celui d'une institution, alors, selon les recherches effectuées en santé publique, on peut obtenir des résultats, à condition de mobiliser des ressources considérables[50]. En fait, dans ces situations, le caractère systématique et la cohésion de la campagne d'information commencent à influer sur la situation primaire des populations locales en ce qui concerne leur comportement sanitaire. Par exemple, il est maintenant établi dans les études sur les médias – par exemple, sur l'impact d'une tentative délibérée d'utiliser les médias pour « améliorer la compréhension de la science par le public » (ce qui équivaut presque invariablement à tenter d'atténuer la perception qu'a le public de certains risques technologiques[51]) – que les messages émanant des médias ne sont pas reçus de façon passive mais sont examinés par le public profane, en fonction de ses connaissances locales, de sa vision du monde et de sa situation de base, de façon beaucoup plus critique que de nombreux « experts » ne se l'imaginent[52]. Lorsque les experts abordent la communication relative aux risques et la persuasion à partir d'hypothèses hiérarchiques ou individualistes, comme ils le font en général, et lorsque les segments de population visés, en raison de leur situation particulière, ne partagent pas ces hypothèses, la persuasion sera inopérante et l'information proposée ne trouvera peut-être même pas preneur[53]. Il ne manque pas d'exemples montrant que des campagnes d'information publique de grande envergure n'ont guère modifié les opinions de la plupart des gens. De fait, c'est désormais un fait bien établi pour les

48. Pour une examen des outils dont disposent les pouvoirs publics, voir Hood C., 1983, *The tools of government*, MacMillan, Basingstoke; Salamon L.M. avec Lund M.S., 1989, *Beyond privatisation: the tools of government action*, Urban Institute Press, Washington DC; Bemelmans-Videc M.-L., Rist R.C. et Vedung E., (dir. publ.), 1998, *Carrots, sticks and sermons: policy instruments and their evaluation*, Transaction Publishers, New Brunswick, New Jersey; Peters B.G. et van Nispen F.K.M., (dir. publ.), 1998, *Public policy instruments: evaluating the tools of public administration*, Edward Elgar, Cheltenham; 6 P, Leat D., Seltzer K. et Stoker G., 1999, *Governing in the round: strategies for holistic government*, Demos, Londres.

49. Linder S.H. et Peters B.G., 1998, 'The study of policy instruments: four schools of thought', dans Peters B.G. et van Nispen F.K.M., (dir. publ.), 1998, *Public policy instruments: evaluating the tools of public administration*, Edward Elgar, Cheltenham, pp. 33-45.

50. Voir par exemple Maccoby N. *et al*, 1977, 'Reducing the risks of cardiovascular disease: effects of a community based campaign on knowledge and behaviour', *Journal of community health*, 3, 1, pp. 100-114.

51. Bien que les professionnels de ce domaine ne s'accordent pas tous à admettre que tel est bien le cas ! voir : Dierkes M. et von Grote C., (dir. publ.), 2000, *Between understanding and trust: the public, science and technology*, Harwood Academic Publishers, Amsterdam.

52. Irwin A. et Wynne B., (dir. publ.), 1996, *Misunderstanding science: the public reconstruction of science and technology*, Cambridge University Press, Cambridge; Irwin A., 1995, *Citizen science: a study of people, expertise and sustainable development*, Routledge, London; Bush J., Moffat S. et Dunn C.F., 2001, 'Keeping the public informed? Public negotiation of air quality information', *Public understanding of science*, 10, 2, pp. 213-229.

53. Schwarz M. et Thompson M., 1990, *Divided we stand: redefining politics, technology and social choice*, University of Pennsylvania Press, Philadelphia; Robins R., 2001, 'Overburdening risk: policy frameworks and the public debate about gene technology', *Public understanding of science*, 10, 1, pp. 19-36.

politologues qui étudient les campagnes électorales depuis les années 40[54], les campagnes électorales n'ont pas d'effet net significatif et souvent pas d'effet très important au niveau individuel, si ce n'est qu'elles peuvent polariser davantage les segments de l'électorat dont les positions sont les plus extrêmes. En général, lorsque les médias accordent à une question de fond une attention qui va au-delà du « cycle normal des médias », on estime qu'ils sont plus efficaces pour centrer l'attention du public sur la question que pour persuader – contrairement au cliché –, pour dire aux citoyens sur quoi ils doivent réfléchir plutôt que pour leur dire quoi penser[55]. Cependant, pour des sujets comme la vie privée, sur lesquels les médias ne concentrent en généralement pas leur attention au-delà du cycle « normal », même cette constatation n'est pas particulièrement prometteuse. Des recherches en psychologie sociale ont démontré que même les personnes que l'on va persuader d'adopter une attitude plus favorable à l'égard de quelque chose ne vont pas pour autant acheter cette chose[56]. Et cela vaudrait en principe autant pour un service respectueux de la vie privée utilisant des TPVP que pour n'importe quoi d'autre. Même lorsque les messages peuvent être maintenus dans la durée, en dépit du « cycle d'attention des médias », on ne saurait s'en remettre aux effets de «cumulatifs» pour amener les gens à modifier leurs préférences[57]. Cette constatation de nature psychologique prend son sens lorsqu'elle est interprétée comme un symptôme de la domination de la situation primaire sur le mode de pensée, telle qu'elle est décrite plus haut. C'est seulement lorsque les individus sont persuadés de modifier la perception qu'ils ont de leur propre identité – autrement dit, selon les termes utilisés ici, lorsqu'une modification peut d'abord être apportée à la situation primaire dans laquelle ils se trouvent – que les psychologues ont observé des effets importants de changement d'attitude, les individus adoptant des attitudes qu'ils estiment cohérentes avec l'identité qu'ils sont en train d'adopter[58]. Pourtant, la plupart des campagnes d'information publique sont axé sur un degré de risque particulier, ou sur un contexte particulier – achat en ligne, consultations et traitements médicaux, services bancaires – plutôt que de façon plus générale sur la situation primaire.

Il ne faut pas pour autant en conclure que les campagnes d'information publique ne peuvent être efficaces qu'en de rares occasions, mais plutôt qu'elles ne donnent pas toujours les résultats escomptés, qu'elles ne parviennent pas forcément à contrer les effets d'autres forces et qu'elles doivent être élaborées avec le plus grand soin, qu'elles doivent être très précisément ciblées plutôt que de portée générale, être centrées sur des risques bien définis, et offrir des raisons très précises d'adopter des solutions données. Il faut aussi qu'elles soient menées sur de longues périodes, qu'elles

---

54. La conclusion originales est de Lazarsfeld P.F., Berelson B. et Gaudet H., 1948, *The people's choice: how the voter makes up his mind in presidential campaigns*, Columbia University Press, New York.

55. O'Guinn T.C. et Faber R.J., 1991, 'Mass communication and consumer behaviour', dans Robertson T.S. et Kassarjian H.H., (dir. publ.), 1991, *Handbook of consumer behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, pp; 349-400, notamment p. 363. Selon une récente étude britannique, l'effet des parti-pris des journaux sur les lecteurs serait beaucoup plus important, tout au moins en ce qui concerne certaines grandes questions, mais les données permettent également de croire que la capacité des lecteurs à exercer leur choix peut être beaucoup plus grande que l'influence des journaux : Lacey C. et Longman D., 1997, *The press as public educator: cultures of understanding, cultures of ignorance*, University of Luton Press, Luton.

56. Zimbardo P.G.et Leippe M.R., 1991, *The psychology of attitude change and social influence*, McGraw Hill, New York.

57. O'Guinn T.C. et Faber R.J., 1991, Mass communication and consumer behaviour', dans Robertson T.S. et Kassarjian H.H., (dir. publ.), 1991, *Handbook of consumer behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, pp. 349-400.

58. Valins D., 1966, 'Cognitive effects of false heart-attack feedback', *Journal of personality and social psychology*, 4, 4, pp. 400-408.

soient en prise sur les valeurs morales fondamentales du segment de public cible, et qu'elles agissent aux niveaux de son sentiment d'identité et sa situation[59].

Les questions de sensibilité aux prix et de prise en compte des coûts de transaction se prêtent à un examen plus bref. Les consommateurs entrant dans la catégorie plus *individualiste* démontreront plus souvent une sensibilité essentiellement proportionnelle et linéaire aux augmentations de prix. On peut prévoir que plus les prix des services intégrant les TPVP dépasseront ceux des services moins respectueux de la vie privée, moins cette catégorie de consommateurs sera disposée à réclamer des services respectueux de la vie privée et les TPVP qui y sont incorporées. C'est surtout pour ce groupe que les courbes classiques de la demande que manient les économistes ont leur utilité. Les groupes plus *enclavés* correspondront à une courbe de sensibilité aux prix plus irrégulière, dans la mesure où ils seront plus susceptibles d'être disposés à payer des prix plus élevés pour la protection de leur vie privée, et où lorsque le coût de la protection de la vie privée dépassera un certain seuil, contrairement aux individualistes, il ne se résigneront pas à y renoncer, mais feront entendre leur voix[60] pour que le régulateur fasse baisser le coût des mécanismes de protection de la vie privée les plus rigoureux auxquels ils sont le plus attachés. La courbe de la demande du quadrant *hiérarchie* sera sensible aux prix mais présentera un coude à un point plus élevé que celle du groupe enclavé, car bien que la régulation soit importante pour les individus de ce groupe, ceux-ci accepteront plus facilement l'idée qu'à l'intérieur d'une tranche définie, il est raisonnable que les organisations pratiquent des prix prenant en compte les coûts. C'est probablement dans la catégorie *isolément* que la sensibilité aux prix sera la plus faible, car les individus de ce groupe ne verront guère d'avantages à tirer des TPVP dans le cadre de leurs relations avec les organisations auxquelles ils ont affaire. La figure 9 illustre les situations qui viennent d'être décrites à l'aide de courbes classiques simplifiées de la demande[61]. Là encore, il convient de se rappeler que les courbes seront souvent différentes selon les contextes.

Afin de comprendre à quel point la demande de consommation de TPVP est susceptible d'être influencée, il reste à prendre en considération la sensibilité des consommateurs aux coûts de transaction non monétaires de la recherche de fournisseurs, de la mobilité entre fournisseurs, ainsi que et du temps et des efforts que les consommateurs y consacrent. Il est à prévoir que les individualistes, là encore, se montreront plutôt sensibles, car pour eux, le temps, c'est vraiment de l'argent. En revanche, ceux qui seront prêts à attribuer à leurs propres temps et efforts la valeur la plus basse pour s'assurer une protection de la vie privée qui leur importe beaucoup seront vraisemblablement les plus enclavés, tandis que la partie la plus « hiérarchique » sera prête à assumer des coûts en temps modérés. La question ne se pose guère pour les isolés/fatalistes en ce qui concerne la vie privée, étant donné que leur intérêt à cet égard est de tout façon très limité. C'est pourquoi les courbes de sensibilité à l'égard des quasi-prix pour la composante non monétaire des coûts de transaction ressembleront beaucoup à celles des différentiels de coûts entre d'une part les services qui respectent la vie privée et utilisent les TPVP, et d'autre part les autres services.

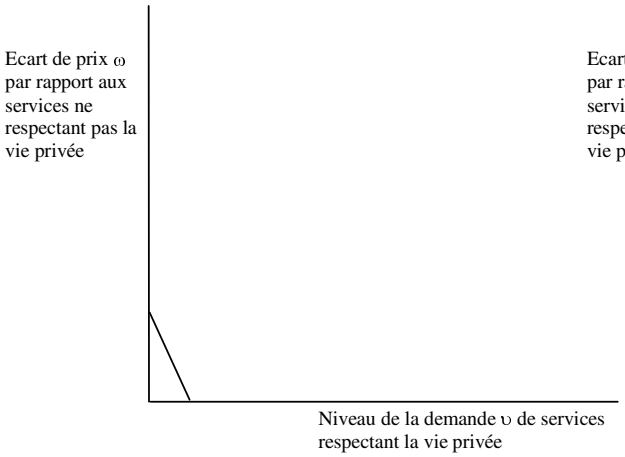
---

59. Weiss J.A. et Tschirhart M., 1994, 'Public information campaigns as policy instruments', *Journal of policy analysis and management*, 13, 1, pp. 82-119.

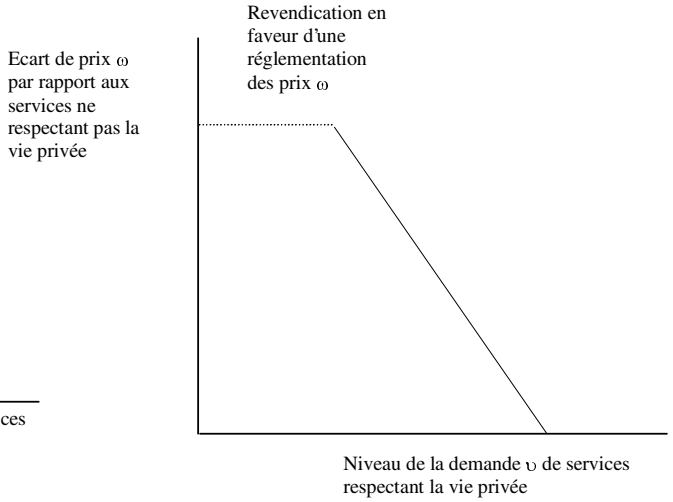
60. Hirschman A.O., 1970, *Exit, voice and loyalty: responses to decline in firms, organisations and states*, Harvard University Press, Cambridge, Massachusetts; Dowding K., John P., Mergoupis T. et van Vugt M., 2000, 'Exit, voice and loyalty: analytic and empirical developments', *European journal of political research*, 37, pp. 469-495.

61. Pour un exemple de représentation de l'impact des quatre situations de base sur les représentations économiques de la demande, voir Wildavsky A., en collaboration avec Fogerty D. et Jeanrenaud C., 1998, 'The concept of externalities is either vacuous or misapplied', dans Wildavsky A., 198, *Culture and social theory*, (dir. publ.) Chai S.-K. et Swedlow B., Transaction Publishers, New Brunswick, New Jersey, pp. 55-84.

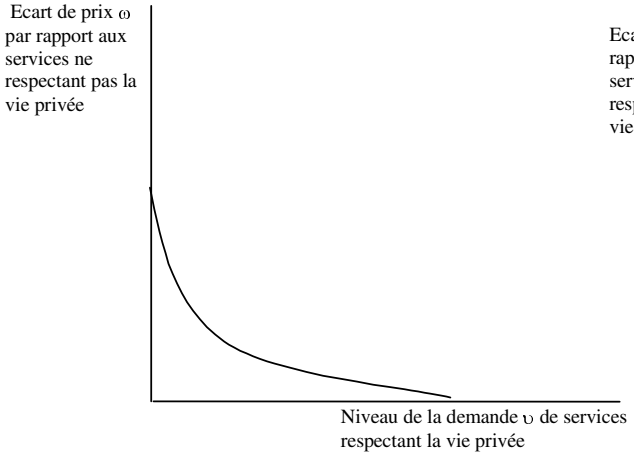
Figure 9. **Courbes de la demande de TPVP chez les consommateurs dans les quatre situations de base**



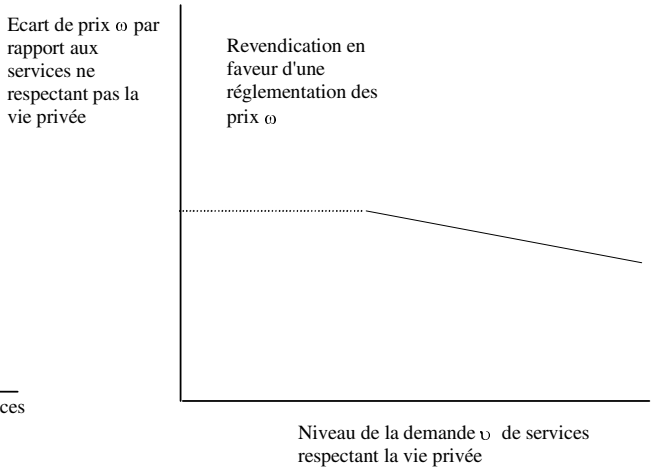
Courbe de la demande des consommateurs isolés/fatalistes -- services utilisant les TPVP



Courbe de la demande des consommateu hiérarchiques -- services utilisant les TPVP



Courbe de la demande des consommateurs individualistes -- services utilisant les TPVP



Courbe de la demande des consommateurs enclavés -- services utilisant les TPVP

Source: Auteur.

Rapprocher les intérêts des entreprises et ceux des consommateurs

Il n'aura pas échappé aux lecteurs que la figure 2 qui décrit les situations de base des entreprises, et la figure 7, qui décrit celles des consommateurs, ont pour point de départ la même analyse. Toutes deux sont des applications de la figure 6. La dimension verticale de la figure 2, qui décrit le degré de structuration monopolistique ou oligopolistique des marchés correspond essentiellement à la dimension « contrainte » de la figure 7 en ce qui concerne les consommateurs, car elle traduit dans quelle mesure le marché est structuré par un certain élément, en l'occurrence la puissance coercitive ou la puissance concurrentielle (régulation sociale). De même, la dimension « surveillance exercée par la collectivité en général » qui apparaît dans la figure 2 et qui explique à la fois la propension à

exploiter et la possibilité d'exploiter est essentiellement la même que la dimension des « liens » dans la figure qui concerne les consommateurs, car elle traduit le degré de responsabilité à l'égard des autres (intégration au groupe social). Cet élément est important car il nous permet de comprendre la dynamique de la relation entre d'une part la capacité et la volonté des entreprises d'offrir des services respectant la vie privée, et d'autre part la capacité et la volonté des consommateurs d'exiger ces mêmes services.

Le cadre institutionnel qui détermine comment les consommateurs percevront les risques et par conséquent quelles seront les préférences de ces derniers en matière de vie privée sera bien sûr lui-même façonné par des aspects de la vie des gens qui dépassent largement leurs relations avec les entreprises. Ces autres aspects institutionnels sont liés aux relations avec les pairs, avec les organismes publics, avec le droit, avec la famille et à bien d'autres encore. Néanmoins, on peut envisager que dans le cadre des processus institutionnels qui régissent les entreprises et les consommateurs, il se crée un processus de *tri* amenant les consommateurs et entreprises de quadrants correspondants à aller les uns à la rencontre des autres.

Les principaux facteurs de tri, dans un quelconque marché, qui permettent à des entreprises et consommateurs présentant des similitudes dans leurs caractéristiques, les cadres institutionnels dans lesquels ils évoluent, les contraintes auxquelles ils sont soumis et leurs préoccupations d'aller les uns vers les autres sont simplement les suivants :

- Dans les marchés concurrentiels, la volonté et la capacité des consommateurs à assumer les coûts de transaction liés à la recherche et à la mobilité jusqu'à ce qu'ils trouvent des fournisseurs en qui ils puissent avoir confiance ou qui leur offrent les protections qu'ils recherchent.
- Dans les marchés non concurrentiels, la capacité et la volonté de mener une action réglementaire, ou la crainte d'une action réglementaire, qui se substituent à l'action des consommateurs aux plans de la recherche et de la mobilité.
- Les stratégies des entreprises, fondées sur l'espoir, qui consistent à investir dans la commercialisation afin de signaler leur présence sur le marché aux consommateurs dont les préférences correspondent à leurs produits et, tout au moins à la marge, à utiliser la publicité et d'autres moyens de persuasion visant à induire chez les consommateurs un changement d'attitude pour influencer leurs préférences.

Le tri n'est certes jamais parfait, car dans les marchés concurrentiels, où d'importants coûts de recherche et de mobilité sont inévitables, il faut un certain temps aux nouveaux consommateurs – qui n'ont pas l'expérience des consommateurs de longue date sortant du marché –, même si leurs préférences sont bien établies (ce qui est souvent loin d'être le cas), pour trouver le secteur qui répond le mieux à leurs préférences.

A quel degré de tri peut-on s'attendre, même dans les conditions les plus favorables ? On peut avancer qu'un degré de tri raisonnable pourra exister tout au plus dans trois des quadrants correspondants. Les entreprises dans le quadrant « sous les projecteurs » pourront peut-être attirer suffisamment de consommateurs « enclavés » ayant des préférences bien arrêtées et ces consommateurs seront de leur côté prêts à assumer les coûts de transaction liés à la recherche et à la mobilité pour quitter d'autres fournisseurs afin de trouver les entreprises désireuses de répondre à leurs préférences. De même, les entreprises les plus dynamiques (« secteur entreprenant ») seront capables de susciter l'intérêt des consommateurs plus individualistes pour la fourchette de ratios prix/protection de la vie privée que leur bouquet de services peut offrir. Là encore, le vaste monde bureaucratique correspondant au secteur « bien régulé » pourrait attirer suffisamment de consommateurs de la

catégorie « hiérarchique » pour que chaque secteur soit viable, même s'il existe une certaine instabilité dans chacun des secteurs parmi les différentes entreprises. Cependant, il existe un secteur d'entreprises et un segment de population de consommateurs pour lesquels le tri est forcément limité. Par définition, le secteur « contrevenant » captera ce qu'il peut, et pas seulement des consommateurs de la catégorie des « isolés-fatalistes », même si ce sont les plus vulnérables ; inversement, les consommateurs de cette dernière catégorie peuvent se retrouver dans n'importe quel secteurs d'entreprises et, encore une fois par définition, ils ne verront guère d'utilité à assumer les coûts de recherche et de mobilité pour changer de secteur, même dans ce scénario de « tri ».

Même advenant à un degré raisonnable de tri sur trois quadrants, il importe de noter que certains conflits peuvent subsister car la correspondance entre les TPVP que les entreprises offrent et celles que les consommateurs recherchent ne sera peut-être pas toujours exacte. La figure 10 montre le degré de correspondance dans un scénario de « tri », en rapprochant les principaux éléments des figures 5 et 8.

Figure 10. **Degré d'adéquation et d'inadéquation dans un scénario de « tri » sur trois quadrants**

Contraintes/barrières à l'entrée

ω

Entreprises: **Secteur « contrevenant »** Les entreprises ne sont susceptibles d'offrir aucune TPVP, mais résiste vigoureusement aux mécanismes de tri	***Consommateurs:*** ***I*solement-fatalisme** [ne pas prendre en compte, car les consommateurs sont passifs et ne réagissent pas aux mécanismes de tri]	***Entreprises:*** **Secteur bien régulé** TPVP les plus susceptibles d'être offertes: *alerte, information* TPVP susceptibles également d'être offertes : *accès de la personne concernée, limitation d'identification, demande de modification de données*	***Consommateurs:*** **Optique hiérarchique** TPVP suscitant le plus d'intérêt: *alerte, information* TPVP suscitant un certain intérêt : *accès de la personne concernée, possibilité de modifier les données, limitation de l'identification*	υ *Liens/ surveillance de la collectivité*
Entreprises: **Secteur entreprenant** TPVP les plus susceptibles d'être offertes: *alerte, information, accès de la personne concernée* TPVP pouvant être offertes également: *limitation de l'identification, demande de modification des données*	***Consommateurs:*** **Individualisme** TPVP suscitant le plus d'intérêt: *accès de la personne concernée, possibilités de modifier les données,* TPVP suscitant un certain intérêt : refus explicite, *information*	***Entreprises:*** **Secteur « sous les projecteurs »** TPVP les plus susceptibles d'être offertes: *alerte, information, accès de la personne concernée, limitation de l'identification, demande de modification des données* TPVP également susceptibles d'être offertes : *consentement, limitation de la collecte, limitation de la destination*	***Consommateurs:*** **Enclave** TPVP suscitant le plus d'intérêt: *consentement explicite, limitation du type de collecte, limitation du contexte de collecte, limitation de l'identification, limitation de la destination, notification* TPVP suscitant un certain intérêt: *accès de la personne concernée*	

Source: Auteur.

Comme on pouvait s'y attendre, c'est dans le secteur « hiérarchique/bien régulé » (quand la réglementation est adéquate) que l'on retrouve le moins de conflits, car c'est là que les consommateurs peuvent le plus facilement s'ajuster à ce que les entreprises, sous les pressions des coûts et des situations, sont les plus susceptibles d'offrir. Cependant, il est tout à fait possible que des consommateurs individualistes réclament un accès plus facile aux demandes de correction de données et davantage de possibilités d'exprimer leur consentement que ce que les entreprises du secteur « entreprenant » trouveront peut-être rentable d'offrir dans les horizons temporels qu'elles privilégient, et il est encore plus probable que les consommateurs enclavés les plus extrêmes exigeront des protections de la vie privée dont le coût sera trop élevé pour que les petites et moyennes entreprises des créneaux spécialisés du secteur « sous les projecteurs » les jugent rentables. Cela cadre avec le raisonnement théorique plus large selon lequel cette zone, tout au moins dans de nombreuses situations, présenterait une nette tendance aux conflits et à la séparation entre fournisseurs et consommateurs[62].

Si par ailleurs il existe des blocages institutionnels au tri – par exemple, si le nombre de consommateurs enclavés est insuffisant pour soutenir un secteur d'entreprises très à l'écoute des consommateurs et capables de répondre à des demandes très exigeantes en matière de protection de la vie privée, ou si les coûts de mobilité d'au moins certains groupes de consommateurs vers le secteur qui pourrait autrement le mieux répondre à leurs préférences sont élevés –, il faut s'attendre à des conflits plus importants. En situation de conflit, un certain nombre d'issues sont possibles. Une issue intéressante est la possibilité que le conflit en lui-même représente un changement sensible par rapport à la situation primaire du consommateur, qui amène ce dernier à changer carrément d'attitude. Le consommateur peut trouver qu'il ajuste son attitude au secteur dans lequel il se trouve, ce qui produit un processus de tri décalé. Le consommateur peut également réagir contre les institutions de ce secteur[63]. Des pressions peuvent s'exercer dans chaque sens. Cependant, on doit s'attendre que dans un marché où la concurrence est limitée et où le consommateur ne dispose guère d'autre choix que d'utiliser le service offert par l'opérateur historique, il subira des pressions plus fortes pour adapter son attitude au secteur dans lequel se trouve le monopole. Dans un cas, nous nous trouvons en présence d'un exemple de persuasion du consommateur par l'entreprise, dans l'autre, c'est l'inverse. Comme cela a été précisément noté ci-dessus en ce qui concerne les campagnes d'information publique, il n'est pas possible de prédire comment évoluera l'attitude du consommateur qui aura quitté son point de référence dans l'organisation sociale, que ce soit délibérément, à la suite d'une action des pouvoirs publics ou pour d'autres raisons.

L'une des questions clés du point de vue de la politique gouvernementale est de savoir s'il faut avoir comme objectif de lever les obstacles au tri qui sont liés au cadre institutionnel et au marché. Selon le raisonnement développé ici, si l'on veut réduire les conflits – toutes choses étant égales par ailleurs (telles que le coût et le risque associés à la levée des obstacles, et la possibilité de conséquences inattendues) –, cela pourrait se justifier.

---

62. Pour l'argument théorique plus général concernant la séparation et le conflit dans ce secteur, voir Thompson M., Ellis R.J. et Wildavsky A., 1990, *Cultural theory*, Westview Press, Boulder, Colorado.

63. Pour une étude de l'éventail d'issues possibles, voir les pistes proposées dans « Theory of surprise » dans Thompson M., Ellis R.J. et Wildavsky A., 1990, *Cultural theory*, Westview Press, Boulder, Colorado, ch. 5.

Conclusion

L'argument développé dans la présente étude est que l'on dispose d'une certaine marge pour persuader les entreprises et les consommateurs de s'intéresser davantage, respectivement, à offrir et à réclamer des services bénéficiant des technologies protectrices de la vie privée, même si ces services sont légèrement plus coûteux que les autres. Cependant, nous avons vu que les possibilités de persuasion étaient limitées et que les pouvoirs publics et les mouvements qui militent en faveur de l'utilisation des TPVP devaient en être conscients. Il est possible de présenter certains types de TPVP de façon à les rendre plus attrayantes pour les entreprises, comme pour les consommateurs, dans certains types de situation. Si l'on peut travailler dans le sens des contraintes, des contextes institutionnels, des hypothèses de base et des perspectives des entreprises et des consommateurs dans ces situations, et si l'on peut parvenir à une appréciation révélatrice de ce qui est susceptible de les intéresser, alors il sera peut-être possible de cibler la communication concernant les TPVP sur des publics assez rigoureusement définis et d'obtenir des résultats.

Par ailleurs, il serait vain d'appliquer à tout le monde les mêmes « recettes de persuasion » ou de croire que n'importe quelle entreprise ou n'importe quel consommateur peut être persuadé de s'intéresser à n'importe quel type de protection contre n'importe quel risque d'atteinte importante à la vie privée, et encore moins à n'importe quel coût. L'étude préconise une certaine modestie dans l'ambition des responsables politiques : le début de la sagesse est d'accepter que l'échec d'une politique sera d'autant plus probable que ses objectifs seront ambitieux, en termes de public visé et d'objet de la persuasion envisagée. En outre, la persuasion la plus efficace induit des changements d'attitude d'une portée relativement limitée. Les métamorphoses radicales sont rares et ne sont en général pas le résultat de l'influence exercée par les pouvoirs publics.

Les aspirants stratèges de la persuasion auront donc pour première tâche de comprendre comment les entreprises et les consommateurs sont segmentés selon les situations dans lesquelles ils se trouvent, pour ensuite en dégager une évaluation des types de TPVP au sujet desquelles une persuasion est possible. Il leur faudra après parvenir à une compréhension claire des perceptions de base dans lesquelles ces TPVP devront trouver leur pertinence. Enfin, il leur restera à déterminer de quels outils ils disposent pour atteindre chacun de leurs publics cibles.

La conclusion encourageante qui se dégage de la présente étude, c'est que certains types de protection de la vie privée revêtent une certaine importance dans des situations très variées. La conclusion qui est moins encourageante, en revanche, c'est que les responsables de l'action gouvernementale et les stratèges de la persuasion ont devant eux une tâche énorme pour déterminer de façon plus précise jusqu'où la protection de la vie privée importe, a de l'importance, et pour qui.

RÉFÉRENCES

Burkert, Herbert (1997), « Privacy-Enhancing Technologies : Typology, Critique, Vision » dans P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge.

Commissaire à l'information et à la vie privée de l'Ontario et *Registratiekamer* (1995), « Privacy-Enhancing Technologies : The Path to Anonymity », août.

Marx, Gary T. (1990), « Privacy and Technology », http://web.mit.edu/gtmarx/www/privantt.html.

OCDE (1980), *Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, OCDE, Paris, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

UE (Union Européenne) (2000), « Document de travail : le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », Groupe de travail sur la protection des données établi par l'article 29 de la directive 95/46/CE, , 21 novembre 2000, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf.

Chapitre 14

CONTRATS RÉGISSANT LES FLUX TRANSFRONTIÈRES DE DONNÉES DANS LE CADRE PLUS GÉNÉRAL DES MÉCANISMES DE PROTECTION DE LA VIE PRIVÉE SUR LES RÉSEAUX MONDIAUX

Ce chapitre examine l'utilisation de solutions contractuelles pour les flux transfrontières de données (FTD), dans le cadre plus général des mécanismes de protection de la vie privée et prend acte de l'évolution de l'environnement dans lequel s'inscrivent les FTD, ainsi que de l'impact de l'infrastructure mondiale de l'information (IMI) sur le traitement et la transmission des données à caractère personnel. Le rapport examine les deux grandes catégories de flux transfrontières de données : les flux interentreprises et les flux de consommateur à entreprise. Il met en lumière les problèmes que pose aux communications en ligne, et notamment aux communications électroniques consommateur-entreprise, l'application de l'analyse et des structures propres aux contrats. Le rapport souligne également la nécessité de développer des mécanismes de règlement des différends qui soient spécifiques aux échanges électroniques consommateur-entreprise. Lorsqu'il y a lieu, il suggère telle ou telle initiative pour promouvoir une utilisation plus large des solutions contractuelles pour la protection de la vie privée dans le cas de FTD liés aux communications en ligne.

Chapitre 14

CONTRATS RÉGISSANT LES FLUX TRANSFRONTIÈRES DE DONNÉES DANS LE CADRE PLUS GÉNÉRAL DES MÉCANISMES DE PROTECTION DE LA VIE PRIVÉE SUR LES RÉSEAUX MONDIAUX

Points principaux

Critères fondamentaux à respecter dans les solutions contractuelles

Un certain nombre de critères fondamentaux propres aux contrats de protection de la vie privée, ainsi que d'autres éléments pertinents, tels que ceux liés à l'exécution ou autres critères accessoires et autres mécanismes de protection, sont importants pour favoriser le respect de la vie privée. Parmi les critères fondamentaux, figurent les règles substantielles – dont les principes énoncés dans les Lignes directrices de l'OCDE sur la vie privée constituent le seuil minimum –, qui fixent les obligations des parties en matière de protection de la vie privée ; l'existence d'une procédure viable pour le dépôt et l'instruction des plaintes ainsi que des mécanismes appropriés de règlement des différends. Les règles substantielles proposées dans ce rapport ont pour objet de servir de cadre commun de référence pour la discussion et l'étude des solutions existants ou en cours de développement, de l'expérience acquise à ce jour et des travaux ultérieurs possibles relatifs à l'approche contractuelle.

Modèles contractuels existants ou à l'étude

Le rapport fait ressortir l'intérêt historique porté aux contrats FTD interentreprises et passe en revue les contrats types, notamment les clauses modèles élaborées par la Chambre de commerce internationale (CCI), ainsi que les initiatives en cours visant à prendre des codes de conduite et des normes professionnelles officielles comme base contractuelle. Il attire l'attention sur la souplesse des contrats types, dont on peut modifier les dispositions pour prendre en compte des catégories professionnelles/sectorielles ainsi que des circonstances particulières, comme des données spécifiques ou l'utilisation d'un support particulier. Tout en identifiant certaines contraintes liées à l'utilisation de contrats interentreprises, la discussion aboutit à la conclusion que les contrats interentreprises types peuvent répondre aux exigences en matière de protection de la vie privée, indépendamment du fait que les données soient transmises en ligne ou hors ligne, en particulier si ces contrats sont complétés par des mesures accessoires, telles que l'information sur les mesures de protection de la vie privée donnée à la personne concernée au moment de la collecte de ses données.

Recours du particulier dans les contrats interentreprises

En cas de rupture du contrat, les parties au contrat de même que généralement des tiers bénéficiaires du contrat disposent de voies de recours. Pour faire en sorte que les personnes concernées par le traitement de leurs données aient les moyens de faire appliquer les clauses d'un contrat FTD interentreprises, le contrat type de la CCI prévoit que toute personne concernée, ou Autorité de protection des données agissant au nom de cette personne, a le droit de poursuivre en justice, pour rupture de contrat, l'exportateur de données en cas de manquement par l'importateur des données aux

clauses du contrat. Cela permet de s'assurer que la personne concernée peut engager la responsabilité d'une partie au contrat (l'exportateur de données) dans son pays d'origine. Même si certains craignent que cette possibilité de recours soit insuffisante pour garantir le respect des clauses du contrat par l'importateur des données, il est important de noter que la personne concernée peut également bénéficier de droits exécutoires par l'effet d'autres infrastructures de protection de la vie privée, comme la loi ou une autorégulation efficace.

Questions soulevées par les interactions entre consommateurs et entreprises

Le rapport examine les caractéristiques des échanges consommateur-entreprise en ligne, analyse les problèmes soulevé par le recours aux voies contractuelles dans ces échanges et démontre que des problèmes de protection de la vie privée peuvent se poser avant la conclusion d'un contrat, qui nécessitent alors la mise en jeu d'autres mécanismes de protection de la vie privée. A cet égard, le rapport suggère que les politiques de protection de la vie privée, et les déclarations faisant état de ces politiques, ont un rôle essentiel à jouer et qu'elles peuvent fournir le moyen de transformer une politique de protection de la vie privée en un engagement contraignant. Les organismes de protection des consommateurs, les organisations tierces et des mécanismes de vérification efficaces internes sont appelés à jouer un rôle important dans l'offre de services et d'outils de certification ou de contrôle.

Nécessité de mettre en place des mécanismes appropriés de règlement des litiges

La question du règlement des litiges est identifiée comme primordiale pour instaurer le climat de confiance nécessaire à l'utilisation des réseaux mondiaux par les entreprises et les consommateurs. Il est suggéré que les procédures de dépôt et d'instruction des plaintes ainsi que les voies d'exécution devraient être développées pour tenir compte des spécificités des transferts électroniques en ligne consommateur-entreprise. A cet égard, les méthodes classiques de règlement des litiges sont examinées en mettant leurs atouts et limites en lumière. D'autres mécanismes de règlement des différends en ligne qui sont actuellement expérimentés, sont également présentés.

Initiatives futures

Enfin, le rapport tire un certain nombre de conclusions de l'examen des thèmes susmentionnés. Il met en évidence les questions particulières qui doivent être résolues pour réaliser l'objectif qui est de protéger la vie privée. Le rapport tend également à identifier les initiatives qui pourraient favoriser le recours aux solutions contractuelles, d'autres questions qui nécessitent un examen ou des travaux plus approfondis, et les initiatives qui pourraient faire progresser les travaux réalisés à ce jour sur l'utilisation de solutions contractuelles, notamment pour les échanges et les interactions consommateur-entreprise en ligne. Le rapport souligne enfin la nécessité de mettre en place des mécanismes de règlement des litiges qui soient spécialement conçus pour les communications électroniques entre les consommateurs et les entreprises.

Les quatre thèmes ci-après se dégagent du rapport :

- L'importance de la sensibilisation aux questions de protection de la vie privée et la nécessité de proposer des outils éducatifs :

  Conformément au principe de transparence énoncé dans les Lignes directrices de l'OCDE sur la protection de la vie privée, il convient de privilégier continuellement des mesures systémiques pour améliorer l'affichage des déclarations de politique de

protection de la vie privée et les procédures d'abstention du consentement, telles que le générateur de déclaration de politique de protection de la vie privée de l'OCDE. Il pourrait être envisagé de créer une page spécifique d'informations pour cataloguer les ressources qui peuvent fournir des informations complémentaires sur les législations relatives à la vie privée, les mécanismes d'autorégulation, etc.

- Une illustration des moyens permettant d'élaborer des « engagements » de protection de la vie privée pour les transferts consommateur-entreprise en ligne et de les faire respecter :

  Les déclarations de politique de protection de la vie privée pourraient servir à l'avenir de point de départ pour définir les termes et les conditions régissant les transactions sur un site Web. Elles pourraient en particulier porter sur le fond de la protection de la vie privée, les mesures de vérification ou les processus de certification applicables au site Web. Ces conditions seraient notifiées au consommateur avant la conclusion du contrat.

- Les diverses évolutions intervenant au niveau international qui nécessitent un suivi et une collaboration ultérieure :

  On observe au niveau international de nombreuses évolutions, qu'il importe de suivre afin d'être en mesure d'en tirer des enseignements pour la mise en œuvre de solutions contractuelles et de mesures complémentaires pour protéger la vie privée. Ces évolutions comprennent tous travaux à venir relatifs aux clauses modèles de la CCI et aux divers projets menés un peu partout dans le monde en vue d'étudier des mécanismes de règlement des litiges en ligne.

- La possibilité d'élaborer un cadre pour un règlement alternatif efficace des litiges concernant les transferts en ligne consommateur-entreprise.

Introduction

Mondialisation des transferts de données et impact de l'Internet

La mondialisation de l'économie et le perfectionnement croissant des technologies de l'information et de la communication favorisent la mondialisation des transferts de données internationaux. Les systèmes d'information internationaux constituent l'infrastructure de base de toute compagnie multinationale pour ses transactions de biens et de services. De plus en plus d'entreprises effectuent des transferts internationaux de données. Les organisations qui collectent et traitent les données à caractère personnel ont désormais les moyens de réutiliser ces données et de les transmettre à une échelle sans précédent. Il peut s'agir de FTD de gros volume (des bases de données, par exemple), ou de collectes ponctuelles multiples à l'occasion de certaines activités, telles que la navigation sur l'Internet.

Le réseau de réseaux qui forme l'infrastructure mondiale de l'information, facilite cette mutation dans les flux transfrontières de données. L'infrastructure mondiale de l'information implique l'interconnexion des « autoroutes de l'information », produit de la convergence des technologies des télécommunications et de l'informatique. L'Internet est l'exemple le plus évident de ces réseaux mondiaux. L'environnement en ligne comporte de grands avantages pour les usagers -- information, produits et/ou services personnalisés et interactifs, amélioration de la sécurité et la protection de la vie privée, notamment grâce à l'utilisation de la cryptographie, de pare-feu et de procédures d'identification qui vont bien au-delà de ce qu'elles étaient avant l'avènement du cybercommerce -- mais il pose aussi de nouveaux problèmes de protection de la vie privée.

Confiance des consommateurs et commerce électronique

Dans cet environnement d'échanges mondiaux, les données à caractère personnel prennent une importance économique de plus en plus grande. L'économie de l'information (ou l'économie fondée sur le savoir, comme il est maintenant convenu de la désigner) mobilise une énorme masse d'informations, y compris les données à caractère personnel. L'information est considérée comme un actif marchand essentiel.

La nature du problème a été reconnue à la fois au niveau international et par les gouvernements nationaux, ainsi qu'en attestent les liens qui ont été établis entre construire la confiance du consommateur (par le biais notamment d'une protection efficace de la vie privée) et faciliter le commerce électronique. Cette corrélation a été l'un des thèmes de la Conférence « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial », qui a réuni les pays membres de l'OCDE à Ottawa, en 1998, et au cours de laquelle les gouvernements se sont engagés à assurer la protection de la vie privée sur les réseaux mondiaux et notamment à favoriser l'utilisation et le développement de solutions contractuelles types pour les FTD en ligne.

Rôle des contrats dans le cadre plus général des mécanismes de protection de la vie privée

Au niveau international, il existe, pour renforcer la protection de la vie privée, une grande diversité de mécanismes : législations spécifiques, autorégulation (codes de conduite, codes de bonnes pratiques et normes professionnelles officielles), technologies de protection de la vie privée, labellisation, certification et sceaux ou marques qui y sont attachés. Les contrats font partie de ces mécanismes.

Les contrats créent des obligations juridiques. Utilisés pour les FDT, ils peuvent offrir une certaine souplesse et permettent de prendre en compte les différences entre les approches adoptées par les pays à l'égard de la protection des données à caractère personnel dans le contexte des réseaux mondiaux. Les contrats peuvent également constituer une mesure de protection pratique et constructive en l'absence de législation ou d'un cadre d'autorégulation efficace sur la protection des données ou lorsque législations ou dispositions d'autorégulation sont différentes. Ils peuvent aussi être le complément ou le pivot de la conformité à des mesures d'autorégulation ou des dispositions légales. Les termes et conditions des contrats peuvent parfaitement refléter les exigences prévues par certains instruments spécifiques de protection de la vie privée.

Ainsi, certains instruments exigent un traitement particulier pour les FTD. La Partie Trois des « Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel » (Lignes directrices de l'OCDE sur la protection de la vie privée) stipule notamment que les pays membres ont le droit d'imposer des restrictions aux transferts de certaines catégories de données à caractère personnel, soumises à un contrôle spécifique dans leur législation interne, aux pays membres n'assurant pas une protection équivalente. Ces restrictions doivent être conciliées avec la volonté déclarée de l'OCDE de favoriser la libre circulation de l'information entre les pays membres et éviter la création d'obstacles injustifiés au développement de leurs relations économiques et sociales.

L'article 12 de la Convention du Conseil de l'Europe pour la protection des individus à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) et l'article 9 des Principes directeurs des Nations unies pour la réglementation des fichiers personnels informatisés (1990) comportent des dispositions de même nature. La directive européenne relative à la protection des données (Directive 95/46/CE) dispose aussi, dans son article 25 (premier paragraphe), que les

transferts de données d'un État membre vers un pays tiers ne peuvent avoir lieu que si celui-ci assure un niveau de protection adéquat. L'article 26, paragraphe 2, de cette directive admet explicitement la possibilité d'utiliser des contrats afin d'assurer aux données transférées d'un pays à un autre le niveau de protection adéquat visé par la directive. En outre, certains instruments nationaux comportent, depuis des années, des dispositions particulières applicables aux FTD (c'est le cas notamment en Allemagne et en France).

I. Critères fondamentaux à respecter dans les solutions contractuelles

Toute discussion relative aux solutions contractuelles de protection de la vie privée et des données à caractère personnel est d'autant plus utile qu'elle s'appuie sur une identité de vues quant aux objectifs visés par ce type de solutions. Pour que se dégage cette identité de vues, il importe de comprendre le rôle des contrats dans le cadre plus général des mécanismes de protection de la vie privée, mais aussi le rôle de ceux des éléments d'une solution contractuelle qui sont jugés importants du point de vue de la protection de la vie privée. S'agissant des contrats FTD, il peut être utile de dresser la liste de ceux de ces éléments qui sont nécessaires pour produire une solution contractuelle efficace. Toute discussion doit également prendre en compte les critères accessoires ou les caractéristiques propres au cadre de protection dans lequel s'insère le contrat FTD.

Nécessité d'une référence à un cadre commun de règles substantielles

Les parties à un contrat FTD doivent veiller à ce qu'il comporte des règles substantielles de protection des données applicables au transfert de données en question. Ces règles peuvent être la réitération des principes énoncés dans les Lignes directrices de l'OCDE sur la protection de la vie privée, mais aussi s'inspirer d'un autre instrument énonçant des principes équivalents. Les solutions contractuelles de protection de la vie privée peuvent assurer un niveau de protection adéquat, tel que formulé dans les Lignes directrices de l'OCDE. Cet objectif est précisé par la recherche d'équilibre formulée en préambule des Lignes directrices :

« Reconnaissant :

> *que, bien que les législations et politiques nationales puissent différer, il est de l'intérêt commun des pays membres de protéger la vie privée et les libertés individuelles et de concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information ;*
>
> *que le traitement automatique et les flux transfrontières de données à caractère personnel créent de nouvelles formes de relations entre pays et exigent l'instauration de règles et pratiques compatibles ;*
>
> *que les flux transfrontières de données à caractère personnel contribuent au développement économique et social ;*
>
> *que les droits internes concernant la protection de la vie privée et les flux transfrontières de données à caractère personnel sont susceptibles d'entraver ces flux transfrontières.*

Résolu à favoriser la libre circulation de l'information entre les pays membres et à éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre ces pays ».

Les principes[1] énoncés dans les Lignes directrices de l'OCDE traduisent un consensus sur les critères et objectifs fondamentaux relatifs à la protection de la vie privée, et établissent un équilibre approprié entre une protection efficace de la vie privée et la libre circulation de l'information. Cependant, le niveau de protection adéquat peut également être assuré dans le cadre d'autres législations ou dispositifs d'autorégulation nationaux basés sur les Lignes directrices de l'OCDE.

Pour un exportateur européen, il pourrait s'agir des critères définis par la Directive européenne ou des accords entre la Commission européenne et des pays tiers. A cet égard, le groupe de travail consultatif de l'Union européenne sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel (groupe de travail de l'article 29) a rédigé un document de travail[2] sur l'application de dispositions contractuelles aux FTD vers des pays tiers. Dans ce document, le groupe de travail de l'article 29 précise le sens de l'expression « garanties adéquates » *(adequate safeguards)* utilisée dans la directive européenne en ce qui concerne les contrats FTD, et reconnaît que les droits et obligations définis dans les Lignes directrices de l'OCDE, qui ne sont pas différents d'autres instruments internationaux traduisent un consensus quant au contenu des règles de protection des données dont l'ampleur dépasse largement le cadre des 15 pays de l'Union.

Il pourrait également être inférieur à des codes de conduite et des normes professionnelles. On constate depuis quelques années des initiatives d'autorégulation tendant à l'adoption de ce type d'instruments en vue d'assurer la protection de la vie privée. Ces initiatives peuvent prendre la forme de codes de conduite (ou de bonnes pratiques) spécifiques à une profession ou à un secteur économique. Ces codes peuvent être administrés par l'organisme professionnel ou sectoriel compétent qui dispose du pouvoir d'imposer des sanctions à ses membres, ou leur mise en œuvre peut être contrôlée par des organismes d'autorégulation du secteur privé, comme cela se fait aux États-Unis. Ils constituent une sorte de contrat sectoriel entre les membres participants. Dans certains pays comme la Nouvelle-Zélande, l'autorité de tutelle chargée de la protection des données est compétente à l'égard du code de protection de la vie privée et peut lui donner force de loi. De telles normes pourraient être incorporées dans des contrats FTD. Il existe une autre forme de normes consensuelles, telles celles qui sont élaborées par les organismes de normalisation officiels au niveau national. Citons à titre d'exemple la norme canadienne CAN/CSA-Q830-96. Cette approche est particulièrement indiquée pour les pays ne disposant d'aucune législation relative à la protection de la vie privée ou lorsque les FTD du secteur privé ne sont pas réglementés du tout. La démarche normalisatrice permet ainsi de disposer d'un ensemble minimum de principes, d'une méthode de mise en œuvre et d'une structure possible pour appliquer une mesure de protection.

La flexibilité que confèrent les clauses modèles de la CCI, qui prennent en compte le fait que l'approche de la protection de la vie privée varie d'un pays à l'autre, permet d'établir des passerelles entre ces approches sur la base du consensus exprimé dans les Lignes directrices de l'OCDE. Les clauses modèles stipulent ainsi que l'importateur de données est tenu de respecter les règles de protection des données applicables dans le pays où l'exportateur de données est établi ou, le cas échéant, un ensemble de principes jugés adéquat en cas de flux transfrontières de données. A titre d'exemple, cette obligation implique que l'exportateur (et partant, l'importateur) est tenu de respecter un ensemble précis de principes de protection de la vie privée -- par exemple, ceux prescrits par la législation de Nouvelle-Zélande ou par celle de Hong Kong, Chine (s'il s'agit du pays où l'exportateur est établi). A l'inverse, il se peut que les obligations des parties au contrat seraient moindre lorsque la réglementation sur la protection de la vie privée est moins complète, ou inexistante. Indépendamment du stade de développement du droit applicable en matière de protection de la vie privée, les clauses modèles comportent une obligation distincte, qui interdit de transférer et de reconduire des données sans le consentement de l'exportateur initial. Cette clause assure un niveau de protection minimum appropriée.

Nécessité d'assurer le respect des règles substantielles

Le deuxième critère important pour qu'un contrat assure une protection effective de la vie privée repose sur la nécessité de veiller à l'application des règles substantielles qu'il contient. Ce critère est conforme au principe de responsabilité énoncé dans les Lignes directrices de l'OCDE sur la politique de la vie privée, selon lequel « tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés (…) ». Les Lignes directrices disposent également que :

> « *Les pays membres devraient notamment s'efforcer :*
> *(…)*
> *(d) d'instituer des sanctions et des recours appropriés en cas d'inobservation des mesures mettant en œuvre les principes énoncés dans les Parties Deux et Trois ;(…) »*

Des critères pour mesurer l'efficacité d'un dispositif de protection des données ont été proposés, par exemple, par le groupe de travail de l'article 29, qui a défini les trois critères généraux ci-après :

- La capacité du système à assurer un bon niveau de conformité aux règles, ce qui suppose des responsables de traitements fortement sensibilisés à leurs obligations, et des personnes concernées ayant conscience de leurs droits ; les moyens de faire valoir ces droits ; l'existence de sanctions efficaces et dissuasives ; l'existence de systèmes de vérification directe par des autorités de contrôle, des vérificateurs ou des responsables officiels indépendants chargés de la protection des données.

- Le niveau d'aide ou de soutien dont bénéficient les personnes concernées dans l'exercice de leurs droits, ce qui suppose des voies de recours rapides et efficaces pour le particulier, ainsi qu'un quelconque mécanisme institutionnel permettant d'instruire les plaintes en toute indépendance.

- L'existence de voies de recours appropriées pour le particulier, ce qui suppose un système de règlement judiciaire ou d'arbitrage. Des mesures appropriées pour assurer le respect des règles de protection de la vie privée peuvent être inscrites dans un contrat. Le contrat type de la CCI, par exemple, confère à la personne concernée ou à l'autorité chargée de la protection de la vie privée le droit d'agir contre l'exportateur de données dans les conditions prévues par le droit applicable. Ce dernier peut ensuite réclamer une indemnisation à l'importateur de données pour violation du contrat.

Une autre approche est proposée dans le projet de document de discussion des États-Unis de janvier 1998 intitulé *Elements for Effective Self-Regulation for Protection of Privacy*[3]. Dans ce document, il est précisé que pour être efficace un régime d'autorégulation pour la protection de la vie privée ne doit pas se limiter à l'énoncé de politiques ou principes à caractère général. Pour être efficace, l'autorégulation doit s'appuyer sur des règles substantielles et sur des moyens destinés à garantir que les consommateurs connaissent les règles, que les entreprises les respectent et que les consommateurs disposent de voies de recours appropriées quand le non-respect des règles leur cause un préjudice.

S'agissant des mécanismes d'application, un régime efficace d'autorégulation doit comporter de tels mécanismes pour assurer le respect des règles et offrir des voies de recours appropriées pour les parties lésées, en cas de non-respect des règles. Ces mécanismes sont essentiels pour permettre aux consommateurs d'exercer leurs droits en matière de protection de la vie privée et doivent en conséquent être facilement accessibles et abordables pour les consommateurs. Ces mécanismes

peuvent prendre des formes diverses et il est possible que les entreprises doivent en utiliser plusieurs selon la nature de leur activité et celle des informations qu'elles recueillent et utilisent.

Ces outils d'application incluent notamment les voies de recours ouvertes au consommateur (mécanismes permettant de donner suite à leurs réclamations), la vérification (attestation que les affirmations de l'entreprise concernant ses pratiques en matière de vie privée et leur mise en œuvre sont sincères et conformes à la réalité) et les conséquences (le non-respect de pratiques loyales en matière d'information ne doit pas rester sans conséquences). On peut citer le retrait du droit d'utiliser un sceau ou un logo de certification, la publication du nom du contrevenant sur une liste de « fraudeurs » publiquement accessible ou l'exclusion par l'association professionnelle à laquelle il appartient. Les contrevenants devraient être tenus d'assumer les coûts engagés pour démontrer qu'ils n'ont pas respecté les règles. Au bout du compte, les sanctions devraient être suffisamment sévères pour être significatives et suffisamment rapides pour montrer aux consommateurs que leurs intérêts sont défendus avec diligence. Lorsque des entreprises affirment respecter certains principes de protection de la vie privée alors qu'en réalité elles ne le font pas, elles s'exposent à des poursuites pour pratiques déloyales et à des sanctions de la part de la *Federal Trade Commission*).

On trouve encore une autre approche dans les documents pour consultation du Gouvernement australien relatifs à la protection de la vie privée dans le secteur privé, et notamment le document d'information publié en septembre 1999. De nombreux facteurs, et notamment les inquiétudes en matière de vie privée qu'éprouvent de nombreuses personnes du fait du commerce électronique, ont influé sur la décision du gouvernement d'élaborer un cadre législatif national pour la protection de la vie privée basé sur les *National Principles for the Fair Handling of Personal Information (National Principles)* publiés par le *Privacy Commissioner* (loi fédérale *Privacy Act* 1988) est le texte législatif principal régissant la protection de la vie privée dans le secteur public fédéral en Australie) en février 1998, après une consultation approfondie des entreprises et des consommateurs.

Schématiquement, cette législation tend à émettre la reconnaissance de codes d'autorégulation pour la protection de la vie privée étayés par des principes législatifs applicables par défaut et par un régime de traitement des réclamations applicables. Le *Privacy Commissioner* est appelé à jouer un rôle majeur dans ce dispositif. Il mènera une action générale de promotion et de supervision du secteur privé, que celui soit ou non couvert par un code. Le *Privacy Commissioner* sera chargé d'approuver les codes relatifs à la vie privée, de fournir aide et conseils aux organisations, d'instruire certaines réclamations et d'une manière générale de faire connaître et comprendre le dispositif. Comme cela est actuellement le cas dans le cadre des attributions limitées du *Privacy Commissioner* à l'égard du secteur privé, les décisions prises par le *Commissioner* ou par un organisme de règlement des litiges prévu par un code, suite à une réclamation, pourront faire l'objet d'une procédure d'exécution forcée devant la Cour fédérale de l'Australie *(Federal Court of Australia).*

Une autre approche à mentionner est celle adoptée par le Japon. Pour assurer la protection des données à caractère personnel par les entreprises, le Ministère du commerce international et de l'industrie (MITI) a publié des Lignes directrices types pour les entreprises intitulées « Lignes directrices relatives à la protection des données à caractère personnel traitées par ordinateur dans le secteur privé » (Lignes directrices du MITI). Le ministère des Postes et Télécommunications (MPT) a également diffusé des lignes directrices pour les services de télécommunications intitulées « Lignes directrices relatives à la protection des données à caractère personnel dans les entreprises de télécommunications » (Lignes directrices du MPT). De plus, en mars 1999, pour encourager la bonne gestion de la protection des données à caractère personnel par chaque entreprise, le MITI a institué la norme JIS Q 15001 « Cahier des charges du programme de respect des dispositions de protection des données à caractère personnel ». La norme JIS Q 15001 impose aux entreprises de se conformer aux exigences suivantes :

- Établissement, mise en œuvre, tenue à jour et publication d'une politique à l'égard du traitement des données à caractère personnel.
- Restriction de la collecte des données à caractère personnel.
- Restriction de l'exploitation et de la divulgation des données à caractère personnel.
- Réception et traitement adéquat de toutes les réclamations et demandes d'aide des personnes concernées.
- Organisation d'audits, etc.

De plus le JIPDEC *(Japan Information Processing Development Center)* délivre des marques de protection de la vie privée après avoir certifié la conformité des entreprises à la norme JIS Q 1005 et aux Lignes directrices du MITI. Si une entreprise bénéficiant de la marque ne respecte pas la norme JIS Q 1005 ou les Lignes directrices du MITI, le JIPDEC demande des explications, peut exiger des améliorations et peut retirer l'octroi de la marque. De même, le Centre d'enregistrement pour la protection de la vie privée, créé par la *Japan Data Communications Association*, enregistre les entreprises de télécommunications qui mettent en œuvre des mesures appropriées pour protéger la vie privée et délivre à ces entreprises une marque de protection des données à caractère personnel.

Conclusions sur les critères contractuels fondamentaux

Les critères de protection de base devant figurer dans des dispositions contractuelles peuvent être résumés de la façon suivante :

- Des règles substantielles fondées sur les principes énoncés dans les Lignes directrices de l'OCDE sur la protection de la vie privée. L'incorporation de ces principes substantiels directement dans le contrat, ou par renvoi à une loi, à des principes ou à des lignes directrices applicables, permet de satisfaire à ce critère.
- Un moyen quelconque pour veiller à l'application du principe de responsabilité et vérifier que les parties s'acquittent de leurs obligations en matière de vie privée[4].
- Un processus viable de recours et d'instruction des plaintes en cas de manquement aux obligations relatives à la protection de la vie privée.
- Des mécanismes appropriés de règlement des litiges pour les parties lésées.

Selon les circonstances particulières d'un transfert de données, le contrat devra contenir des dispositions plus ou moins étoffées que les règles et la procédure susmentionnées. Il pourra en effet se produire que la protection requise soit garantie dans le cadre plus général de la loi ou de l'autorégulation. Un autre élément à considérer serait la prise en compte du risque associé aux données en cause, selon qu'il s'agira de données à caractère public et non sensible, nécessitent une protection moins stricte que ces données sensibles, qui elles exigent au contraire davantage de protection.

II. Modèles contractuels actuellement appliqués ou a l'étude

Transferts de données interentreprises : domaine de prédilection historique

L'idée d'utiliser des contrats régissant les flux transfrontières de données fait son chemin depuis quelque temps. Au début des années 90, les flux de données étaient en majeure partie des flux interentreprises. Ces flux sont de nature très variée et englobent la fourniture ou l'échange de données à caractère personnel entre plusieurs unités ou divisions commerciales d'une même organisation, les

prestations de services en matière de traitement par une entité pour le compte d'une autre, les transferts de données à caractère personnel en tant qu'objet d'une transaction commerciale normale ou accessoire à celle-ci. Les transferts les plus nombreux interviennent dans le domaine des ressources humaines ou concernent l'élément informations financières (banque, assurance, crédit), les informations marketing (marketing direct, réservations auprès des agents de voyages) et celles des organismes du secteur public (police, douanes et autorités fiscales).

De plus en plus, on prend conscience de l'importance des données à caractère personnel en tant que ressource clé de nombreuses entreprises. Bien que l'impact des télécommunications sur les FTD soit parfaitement connu depuis longtemps, l'avènement de l'infrastructure mondiale de l'information (sous la forme d'Internet ou des réseaux Intranet) a des retombées que l'on commence seulement à traiter. Les réseaux mondiaux permettent de collecter, de traiter et de transmettre des données à caractère personnel à une échelle encore inconnue jusque là. Toutefois, lorsque fut amorcé le débat sur les solutions contractuelles en matière de protection des données, les transferts interentreprises plus classiques mobilisèrent l'attention avec, en point d'orgue, l'élaboration du contrat type du Conseil de l'Europe en 1992.

Contrat type du Conseil de l'Europe (1992)

Le « Contrat type du Conseil de l'Europe visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données » est le fruit d'une étude entreprise conjointement par le Conseil de l'Europe, la Commission des Communautés européennes et la Chambre de commerce internationale (CCI). Ce contrat est constitué d'un ensemble de clauses types, conçues pour assurer une protection équivalente dans le contexte des flux transfrontières de données et inspirées de la Convention 108. Utile pour la mise en œuvre de la clause de protection équivalente des lignes directrices de l'OCDE sur la protection de la vie privée, le contrat type du Conseil de l'Europe est également une référence fort utile pour apprécier ce qui peut constituer un niveau de protection adéquat au sens de la directive européenne.

Aux termes du contrat type, la partie transférant les données (le concédant) donne la garantie que les données ont été obtenues et traitées conformément à la législation sur la protection de la vie privée en vigueur dans l'État où elle exerce ses activités. Les clauses types font notamment obligation de garantir que les données ont été obtenues loyalement et licitement, de mentionner les finalités en vue desquelles elles ont été conservées, ainsi que de garantir qu'elles correspondent à leur objet, sont pertinentes et exactes et qu'elles bénéficient d'une autorisation de conservation pour une durée qui doit être précisée.

La partie destinataire (le cessionnaire) s'engage à respecter les mêmes principes que ceux qui sont applicables à l'exportateur des données. En complément de cet engagement, le cessionnaire s'engage à faire usage des données pour les finalités énumérées au contrat, à l'exclusion de toute autre, à protéger les données sensibles selon les modalités prévues dans le droit interne du concédant, à ne pas communiquer les données transférées à des tiers à moins que le contrat ne l'y autorise expressément et à rectifier, effacer et mettre à jour les données, sur instruction du concédant.

Les autres clauses types concernent la responsabilité en cas d'utilisation fautive des données par le cessionnaire, les droits des personnes concernées, le règlement des litiges et la résiliation du contrat. Les seules modalités précises en matière de règlement des litiges concernent l'arbitrage (y compris le recours à l'expertise) ; les clauses types stipulent que les parties « doivent prévoir un système approprié de règlement des conflits »[5]. La question du droit applicable est laissée au libre choix des

parties. Les travaux du Conseil de l'Europe sur les solutions contractuelles ont servi de base aux travaux ultérieurs.

Contrat type révisé de la CCI

La CCI a révisé le contrat type du Conseil de l'Europe de 1992, à la lumière de l'exigence énoncée par la directive européenne de protection adéquate en cas de transfert de données vers des pays tiers. Cette révision prend en compte les commentaires du groupe de travail institué en application de l'article 29 de ladite directive. Les Clauses modèles pour les contrats impliquant des flux transfrontaliers de données sont le fruit de leurs travaux.

Ces clauses modèles ciblent les transferts de données interentreprises hors ligne (c'est-à-dire par des moyens manuels ou matériels) ou en ligne (sur des supports électroniques). Ce dernier mode de transmission est envisagé dans les notes explicatives des clauses. Autre élément important dans ces notes, les concepts énoncés dans les clauses modèles de la CCI devraient être acceptées par des entreprises d'horizons très divers. Plus ces formules et pratiques gagnent en notoriété dans l'ensemble de la communauté économique, plus elles sont acceptées facilement : par conséquent, les clauses modèles ont vocation à être applicables à tout un éventail de transactions interentreprises, notamment celles des petites et moyennes entreprises.

Les clauses modèles semblent suggérer que certains de leurs éléments doivent être ajustés aux conditions particulières d'un FTD. Ainsi est-il fait référence à plusieurs reprises (clauses 2, 3 et 4) à l'importateur de données, qui doit limiter son utilisation ultérieure des données à caractère personnel aux seules finalités notifiées par l'exportateur ou autorisées par la législation du pays où ce dernier est établi. De même est-il prévu l'interdiction de divulguer les données (sous forme d'une interdiction de communication à un tiers ou à un pays tiers) sans le consentement préalable de l'exportateur.

L'important est que ces clauses représentent un modèle et en tant que tel, constituent une base solide sur laquelle peuvent être élaborées ou adaptées les dispositions destinées à refléter les caractéristiques de l'importateur/exportateur de données et de la législation ou du régime juridique régissant la protection des données. Si ces clauses sont reconnues comme satisfaisant au critère de niveau de protection adéquat visé par la directive européenne, les parties au contrat qui les modifieront le feront à leurs risques : si une modification des clauses a pour effet d'abaisser le niveau de protection, les parties ne pourront pas prétendre que les dispositions figurant dans les clauses modifiées sont suffisantes eu égard aux critères fixés par la directive européenne.

Une analyse plus approfondie du contenu et de la cohérence des clauses modèles de la CCI par rapport à la directive européenne dépasserait le cadre du présent rapport. Il n'en reste pas moins que ces clauses ont une valeur significative en ce qu'elles constituent un document ou modèle de base pour l'élaboration de contrats de protection pour les transactions interentreprises. La question du recours des individus dans le cadre de contrats interentreprises est discutée plus avant dans la section 4.

Autres travaux réalisés sur les solutions contractuelles

Un certain nombre d'études et d'initiatives ont été menées dans d'autres enceintes relatives à l'utilisation de contrats types aux transferts de données interentreprises. Il convient de citer notamment : le document de travail adopté le 22 avril 1998 par le groupe de travail de l'article 29 de l'Union européenne, *Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries*, les recommandations formulées par l'*Office of the*

Privacy Commissioner de Hong Kong, Chine dans *Fact Sheet No. 1*, avril 1997, les travaux du Commissaire à l'information et à la vie privée de l'Ontario (Canada), les travaux sur les contrats types pour le commerce électronique de l'UN/CEFACT (Trade/Cefact/1999/crp.5/Rev1) et enfin, le projet de contrats types de l'*American Business 1999* (P&AB). Ce projet est en cours et porte sur l'élaboration d'un modèle de contrat pour les FTD.

Expérience acquise en matière de contrats FTD

Les clauses modèles de la CCI sont utilisées en Europe essentiellement en tant que référence pour élaborer des contrats FTD *ad hoc* et dans les domaines de l'emploi et des ressources humaines. D'autres initiatives contractuelles interentreprises pour la protection de la vie privée ont été mises en avant en tant qu'exemple[6].

Tel est le cas, par exemple, de l'accord signé entre la société des chemins de fer allemands (Deutsche Bahn AG) et la Citibank. En 1994, la Deutsche Bahn AG et la filiale allemande de la Citibank ont produit des cartes de chemin de fer (offrant des réductions aux usagers voyageant souvent en train), qui fonctionnaient également comme des cartes VISA. Ces cartes étant fabriquées par une filiale de la Citibank aux États-Unis, l'accord a suscité d'importants flux transfrontières de données. En réponse à l'inquiétude exprimée par les Allemands eu égard à la protection des données à caractère personnel, les deux parties conclurent un accord sur la protection interterritoriale des données, conférant aux citoyens allemands le même niveau de protection que celui dont ils auraient bénéficié si les cartes avaient été fabriquées en Allemagne. En particulier, cet accord stipulait que le droit allemand était applicable, limitait les transferts de données à des tiers, autorisait les audits sur place, dans les filiales américaines de la Citibank, par les autorités allemandes chargées de la protection des données ; enfin, il tenait la Deutsche Bahn AG et la filiale allemande de la Citibank responsables à l'égard des personnes concernées de toute violation de l'accord par leurs homologues américains.

L'expérience acquise dans le fonctionnement de cet accord Deutsche Bahn/Citibank est très instructive, mais son application à titre de précédent ou de modèle est assez limitée du fait que des solutions contractuelles de ce type ne sont pas facilement transposables à des transferts interentreprises de moindre envergure.

Conclusions sur les modèles actuels

Les travaux internationaux sur les solutions contractuelles interentreprises ont atteint un tournant important. L'expérience acquise dans l'utilisation de ces contrats a permis de dresser une liste relativement détaillée et complète de tous les critères contractuels (sous la forme des clauses modèles de la CCI). De nouveaux progrès sont prévisibles, liés au fait que ces clauses seront reprises et adaptées de plus en plus souvent. L'expérience acquises dans l'utilisation des clauses modèles, et la nécessité d'adapter ou de modifier leurs modalités en fonction de circonstances particulières pourraient faire l'objet d'un suivi et nourrir les travaux sur leur actualisation. Il pourrait être utile d'aborder des variantes ou des versions différentes pour mieux s'adapter à des catégories professionnelles/sectorielles ou des circonstances particulières. Il est indéniable que ces travaux seront poursuivis et que les enseignements tirés d'autres projets en cours constitueront une valeur ajoutée.

Les modèles contractuels interentreprises ne sont pas si sensibles que cela au support utilisé pour le transfert ou la communication des données, ni si tributaires que cela de celui-ci. Les clauses modèles de la CCI peuvent être appliquées aux flux en ligne (électroniques). S'agissant des solutions contractuelles actuellement utilisées ou en cours d'étude, la difficulté réside dans le fait que l'on s'est

attaché en priorité aux transactions interentreprises et que, par voie de conséquence, les avancées pour la mise au point de solutions cohérentes et efficaces pour les FTD consommateur-entreprise n'ont guère été tangibles. Cependant, les choses vont très vite en ce qui concerne les FTD : de nouvelles contraintes et de nouvelles questions doivent maintenant trouver une réponse. Nous y reviendrons dans la section 5.

III. Recours du particulier dans les contrats interentreprises

A ce jour, les travaux relatifs aux contrats de FTD ont pour l'essentiel porté sur les transferts de données interentreprises (comme les clauses modèles de la CCI). L'expérience acquise en matière de contrats interentreprises permet de voir qu'ils peuvent considérablement améliorer les pratiques équitables de traitement de l'information et aider à éviter les restrictions que les différences dans les approches adoptées par les gouvernements des pays membres risquent d'imposer à la circulation transfrontières des données.

Recours du particulier

Un certain nombre de facteurs peuvent influer sur les possibilités de recours du particulier dans le cadre des contrats interentreprises. Les particuliers sont dans une très large mesure tributaires de l'exportateur des données qui, en pratique, agit comme leur représentant pour assurer le niveau de protection requis. Le contrat type de la CCI tente de prendre en compte ces questions en conférant à la personne concernée ou aux autorités chargées de la protection des données un droit d'action contre l'exportateur des données, lequel peut ensuite réclamer un dédommagement à l'importateur de ces données. L'absence de protection de la vie privée dans le cadre d'un contrat reste toutefois un problème dans les pays -- de moins en moins nombreux -- qui ne reconnaissent pas la stipulation pour autrui. Des contrats interentreprises complétés par un cadre juridique ou un dispositif d'autorégulation pour la protection de la vie privée pourraient constituer une alternative pour le recours du particulier. L'affaire des chemins de fer allemands et de la Citibank fournit un exemple d'une telle possibilité.

Obstacles liés à la logistique et aux ressources

Les solutions contractuelles interentreprises *ad hoc* comportent aussi d'autres inconvénients d'ordre logistique et pratique (frais juridiques, temps et ressources nécessaires) que l'utilisation de contrats types permet d'éviter.

Partage des risques et des responsabilités

En ce qui concerne la question de la compétence juridictionnelle et du choix du droit applicable, l'un des préceptes est de structurer le contrat de façon que l'exportateur des données s'assure, en vertu des lois en vigueur dans son pays, que les pratiques de protection des données seront respectées par tout importateur dans quelque pays qu'il se trouve. C'est cette approche qui sous-tend les clauses contractuelles types de la CCI. L'exportateur est responsable du traitement à l'étranger de toute donnée exportée, et la personne concernée est en mesure d'intenter une action dans sa juridiction contre l'exportateur pour non respect par l'importateur de ses obligations en matière de protection de la vie privée.

Vérification et certification

Il pourrait être utile de disposer de certains types de mécanismes de vérification ou de certification, qui permettent de confirmer que la gestion ou le traitement des données sont effectués par l'importateur conformément à ses obligations contractuelles en matière de respect de la vie privée. Toutefois, l'importance que revêtent les mesures de vérification est moindre dès lors que le particulier bénéficie d'un accès facile à un système efficace de protection qui lui assure un recours par le traitement de sa plainte.

Les processus d'inspection et d'audit qu'exige toute mesure de vérification trouvent leur origine dans les contrats interentreprises, mais ils ont été modifiés pour s'adapter aux interactions en ligne entre consommateurs et entreprises dont les caractéristiques sont différentes. Il a notamment été proposé d'utiliser des labels, des sceaux d'approbation, ou d'autres marques de confidentialité attestant de la conformité du site Web aux règles de protection de la vie privée. Les contrats pourraient prévoir la vérification, si elle est jugée nécessaire, en stipulant des arrangements relatifs aux audits et aux inspections ou des mesures de transparence, dans l'intérêt du particulier. La vérification peut mobiliser des ressources considérables et son efficacité dépendra du choix du vérificateur.

Les clauses modèles élaborées par la CCI prévoient que l'importateur des données s'engage à « soumettre ses installations de traitement des données, fichiers de données et documents nécessaires au traitement, aux procédures de vérification et/ou de certification décidées par l'exportateur de données (ou d'autres vérificateurs indépendants ou autorités d'inspection dûment qualifiées qui sont choisis à cet effet par l'exportateur de données et auxquels l'importateur de données n'a pas raisonnablement d'objection à opposer) pour contrôler le respect des garanties et engagements des présentes Clauses » (Clause 4).

Difficulté pour les particuliers d'exercer leurs droits

Les contrats interentreprises qui portent sur le transfert de données à caractère personnel sans que la personne concernée en soit avisée ou ait donné son consentement rendent difficile pour la personne concernée le fait de contester les données la concernant. Si cette difficulté ne remet pas en cause la pertinence du recours aux solutions contractuelles, elle constitue néanmoins une question qui reste à résoudre.

Les points sur lesquels il importe de se pencher sont les suivants : comment le particulier peut-il savoir si des données le concernant sont collectées ou comment peut-il être mis en mesure de consentir à cette collecte (selon le Principe de la limitation en matière de collecte) ? Comment les parties contractantes dans un transfert interentreprises peuvent-elles informer la personne concernée des finalités et des utilisations qui sont faites des données transférées (en vertu du Principe de la spécification des finalités) ? Les personnes concernées se verront-elles offrir le choix quant à l'utilisation ou à la divulgation ultérieures des données la concernant, ou la possibilité de donner son consentement (en vertu du Principe de la limitation de l'utilisation) ? Comme indiqué plus haut, il est possible, pour résoudre ces questions, de s'inspirer de la solution adoptée pour les clauses modèles de la CCI qui donne aux personnes concernées le droit d'agir contre l'exportateur des données.

La solution des clauses modèles de la CCI

Application des lois du pays de l'exportateur des données

Les clauses modèles de la CCI règlent le problème du droit applicable en imposant à l'importateur de données de se conformer soit aux règles de protection des données de l'exportateur, soit à un ensemble de principes considéré comme adéquat pour les données relatives aux citoyens du pays exportateur. Cela répond à l'objet des clauses modèles de la CCI qui est de faciliter les démarches des parties qui souhaitent transférer des données à caractère personnel d'un pays où leur exportation est réglementée vers un pays qui n'assure pas un niveau de protection de ces données considéré comme adéquat par le pays d'origine. Un autre avantage de l'utilisation des clauses modèles de la CCI est de renforcer la protection des informations personnelles transférées dans le cadre du contrat lorsque le pays destinataire n'assure pas de protection effective de la vie privée, ni par la voie législative, ni par des mécanismes d'autorégulation.

Les clauses modèles de la CCI font obligation à l'importateur des données d'octroyer à la personne concernée les mêmes droits que ceux dont elle aurait bénéficié à l'égard de l'exportateur des données avant leur exportation. Cette situation diffère de celle où la personne concernée tient un droit d'agir directement sur le fondement d'un contrat interentreprises. Le contrat de la CCI prévoit que l'importateur des données assume l'obligation de permettre à la personne concernée de contester les données (ce droit étant inscrit dans la législation relative à la protection des données), par exemple en accédant à toute demande d'accès et de correction concernant ces données.

Participation des autorités compétentes

Une autre mesure comprise dans les clauses modèles de la CCI consiste à intégrer le rôle d'aiguillage des plaintes des autorités ou des organismes gouvernementaux de surveillance en matière de protection des données. Ces clauses prévoient que « l'exportateur de données [s'engage à répondre], dans le plus bref délai, aux questions de l'Autorité relatives à l'utilisation des données à caractère personnel (…) ainsi qu'à toute demande d'information des personnes concernées relatives à l'utilisation de leurs données (y compris la question de savoir si elles ont été exportées) et [à fournir] au demandeur les noms de l'importateur de données et du responsable représentant ce dernier qui sera avisé de la demande et qui a été désigné (…) pour répondre aux questions de ses autorités nationales »[7].

Cette mesure sera plus efficace si la personne concernée sait que des données la concernant font l'objet d'un traitement ou sont exportées selon les modalités prévues par le contrat interentreprises. Les règles de protection des données exigeront selon toute probabilité que la personne concernée soit avisée de ce qu'il adviendra des données la concernant et qu'elle dispose d'une possibilité de choix. L'efficacité de cette mesure dépendra aussi de la capacité des autorités nationales de protection des données à répondre rapidement aux demandes effectuées en application d'un contrat CCI.

Participation de la personne concernée

Les dispositions des clauses modèles de la CCI relatives aux mécanismes de règlement des litiges prévoient expressément les situations dans lesquelles les personnes concernées sont impliquées. L'importateur des données accepte de se conformer à la décision de l'autorité chargée d'enquêter en matière de protection de données. Un certain nombre de démarches doivent cependant être entreprises avant d'amorcer le processus de règlement des litiges, notamment la notification et l'instruction de la

plainte. L'importateur de données s'engage, entre autres, à désigner une personne devant répondre aux demandes d'information (et à en aviser l'autorité compétente) ainsi qu'à traiter les plaintes dans les délais prescrits par la législation ou le dispositif d'autorégulation sur la protection des données applicable dans le pays de l'exportateur.

Sanctions et recours

Les clauses modèles de la CCI confèrent aux personnes concernées les mêmes droits que ceux dont elles jouiraient dans le pays de l'exportateur des données. Elles permettent aussi à ce dernier de résilier le contrat, ou d'insister pour que soient détruites ou restituées les données qui sont à l'origine de la plainte de la personne concernée. L'un des éléments identifié dans le cadre des règles substantielles proposées pour les clauses contractuelles de protection de la vie privée (chapitre 2) est la possibilité d'exercer un recours. La réparation des manquements aux règles de protection de la vie privée est une question qui se pose de façon générale aux pouvoirs publics et n'est pas limitée aux seules solutions contractuelles. En cas de rupture de contrat, il est important de noter que les modes de réparation varient selon les pays et leur législation, et incluent notamment l'exécution en nature, la résolution, la restitution ou l'obtention de dommages-intérêts. L'exécution en nature impose à la partie défaillante de s'acquitter de ses obligations conformément au contrat. La résolution rend le contrat nul et non avenu, les parties revenant à la situation antérieure au contrat, tandis que la restitution impose à la partie défaillante de rétablir la partie lésée dans la situation où elle aurait été si le contrat avait été exécuté. Dans de nombreux pays, l'information est traitée comme un élément intangible auquel il est très difficile d'attribuer une valeur. Cela n'est pas sans conséquence car le plaignant, lors de poursuites judiciaires, aura peut-être du mal à prouver qu'il a subi une perte ou un préjudice par suite du non-respect des obligations en matière de protection de la vie privée, et à chiffrer cette perte ou ce préjudice. Il importe toutefois de noter que cette difficulté n'est pas propre aux contrats. Une indemnisation dont le montant serait prédéterminé pourrait être un moyen de réparation en cas de manquement à des obligations contractuelles. Mais il demeurerait peut-être nécessaire de prouver que la somme retenue correspond à une évaluation réelle de la perte subie. Ceci pourrait donner matière à débat.

Nécessité de droits directement opposables en vertu du contrat

Si l'autorité ou l'organisme gouvernemental de surveillance chargé de veiller à la protection des données ne peut intervenir pour que la personne concernée obtienne réparation, l'une des parties peut engager une action contre l'autre pour transgression de ses obligations. La question se pose toutefois de savoir si la personne concernée peut poursuivre la partie défaillante sur le fondement du contrat interentreprises. Dans certaines juridictions, le fait que la personne concernée ne soit pas partie au contrat peut poser une difficulté (pas de « stipulation pour autrui »). Cet obstacle sera bientôt surmonté car bon nombre de pays ont adopté des lois qui reconnaissent le droit d'un tiers bénéficiaire d'une promesse ou d'un autre engagement contractuel, de faire respecter ses obligations par une partie défaillante.

La nécessité de pouvoir se prévaloir de droits directement opposables ne concerne pas uniquement le particulier. Si l'importateur des données retransmet celles-ci à un tiers, il sera peut-être difficile pour l'exportateur de s'assurer que les règles de protection de la vie privée sont respectées. L'exportateur peut imposer à l'importateur certaines restrictions contractuelles, pour limiter tout traitement ultérieur ou réutilisation de données (tel que prévu dans les clauses modèles de la CCI). Cependant, il se peut que l'exportateur rencontre des difficultés pour faire appliquer de telles

restrictions, à moins que le droit régissant le contrat ne lui permette d'engager une action (à titre de tiers bénéficiaire au contrat entre l'importateur des données et le destinataire ultérieur de ces données).

Information du particulier

Information relative à la protection de la vie privée et autres mesures de sensibilisation

La question de savoir comment les exigences relatives à l'information ou au consentement de la personne concernée (comme celles énoncées dans les Lignes directrices de l'OCDE relatives à la protection de la vie privée) peuvent être prises en compte dans le cadre des contrats interentreprises peut être résolue par le recours à des mesures complémentaires qui, sans modifier la formulation ou le contenu du contrat, contribueraient à sensibiliser davantage les personnes concernées aux usages auxquels on destine les données qui les concernent.

Si les exportateurs de données (ou autres intervenants collectant les données) respectent le Principe de l'OCDE de la spécification des finalités au moment de la collecte, les personnes concernées seront mieux informées et par conséquent mieux en mesure d'exercer leur droit d'accès aux données. Ceci pourrait également fonder des poursuites contre un exportateur des données coupable de représentation trompeuse des faits.

Contrat passé directement avec la personne concernée

En ce qui concerne les recours de la personne concernée, le Groupe de travail de l'article 29 de l'Union européenne[8] recommande une solution « tripartite », selon laquelle l'exportateur des données passe avec la personne concernée un contrat distinct au moment de la collecte des données, qui stipule que l'exportateur sera responsable des conséquences du non-respect par l'importateur des principes convenus en matière de protection des données. Ce moyen pourrait être utilisé pour résoudre le problème de l'insuffisance d'information, et l'absence de connexité contractuelle. La personne concernée pourrait être indemnisée par l'exportateur en cas de défaillance de l'importateur. Il appartiendrait à l'exportateur de recouvrer les sommes en dommages-intérêts payables à la personne concernée en intentant une action séparée contre l'importateur pour violation de contrat. Cette suggestion pourrait se révéler utile dans les quelques pays qui ne reconnaissent pas la stipulation pour autrui.

Cette approche tripartite serait indiquée lorsqu'il est possible de prévoir au moment de la collecte de données qu'un FTD se produira ultérieurement. Dans certains cas, il est possible que le contrat avec la personne concernée fasse partie intégrante des conditions habituelles régissant la prestation de services de certaines organisations. Cela irait aussi dans le sens du principe de transparence de l'OCDE, selon lequel la personne concernée doit être informée de ses droits en matière de vie privée. Néanmoins, ces contrats tripartites pourraient se révéler lourds et difficiles à mettre en œuvre.

Les économies d'échelle

Lorsque la quantité de données à transférer est minime, l'utilisation d'un contrat dédié au flux transfrontières de données ne se justifie pas toujours. Il ne semble pas exister de cas largement connu où des contrats FTD *ad hoc* aient été utilisés par une entreprise dans le cadre de ses relations avec une ou plusieurs personnes concernées par le traitement de leurs données.

Conclusions concernant les recours du particulier

Certains ont pu craindre que les contrats interentreprises n'offrent pas de recours au particulier. Bien que les contrats interentreprises ne puissent garantir un recours dans tous les cas, les diverses mesures proposées dans le cadre d'initiatives comme les clauses modèles de la CCI pourraient bien, dans la majorité des cas, offrir une solution adéquate. L'approche contractuelle illustrée par les clauses modèles de la CCI permet à une autorité chargée de la protection des données ou à un organisme de surveillance gouvernemental de jouer un rôle. D'autres types de contrats pourraient proposer un mode de règlement des litiges par le secteur privé.

Les contrats interentreprises soulèvent d'autres difficultés ayant trait à la compétence juridictionnelle et au droit applicable ainsi qu'à l'impact de la directive de l'UE (en particulier en ce qui concerne les exigences relatives au niveau de protection adéquat). Il s'agit là de questions extrêmement complexes, mais qui ont été prises en considération au cours de l'élaboration des clauses types ou clauses modèles.

A certains égards, les questions qui semblent les plus banales et sans intérêt particulier sont celles qui, au plan pratique, comportent le plus de difficultés ; en particulier, les questions comme l'inégalité des ressources entre les parties et la personne concernée ou le manque d'information (prévu dans les Lignes directrices de l'OCDE sur la protection de la vie privée) sur la finalité de la collecte et l'utilisation subséquente des données. A cet égard, certaines recommandations formulées à propos des transferts de données de consommateurs à entreprises pourraient aussi s'appliquer aux contrats interentreprises, telles les mesures mentionnées dans les sections 5 et 6 visant à donner aux personnes concernées un accès à de l'information sur leurs droits ou à des centres spécialisés, à faire une place plus importante aux déclarations de politique de protection de la vie privée, à mettre en place des mécanismes de vérification, et à offrir la possibilité de recourir à prix raisonnable à un mécanisme facilement accessible de règlement des litiges.

IV. Interactions consommateur-entreprise

La présente section porte principalement sur les caractéristiques des transferts de données en ligne entre consommateurs et entreprises, ainsi que sur les effets induits par ces caractéristiques sur l'applicabilité des solutions contractuelles aux transferts consommateurs-entreprises sur l'Internet. Sont également examinés les mécanismes qui pourraient être modifiés, ou développés, pour améliorer les pratiques en matière de protection de la vie privée et protéger ainsi les renseignements personnels collectés sur le Web.

Impact de l'Internet sur la vie privée

Avant l'Internet, les consommateurs et les entreprises qui étaient situés dans des juridictions différentes avaient très peu de contacts directs. Les particuliers pouvaient acheter des produits ou services à l'étranger pendant leurs vacances, mais la plupart du temps les transactions d'un État à l'autre avaient lieu par l'intermédiaire d'une organisation ayant pignon sur rue dans la juridiction du consommateur (par exemple, compagnie aérienne ou société émettrice de cartes de crédit).

L'essor du commerce électronique a modifié cet état de choses, notamment en ce qui concerne les contrats portant sur les services et produits d'information (comme les livres, les disques compacts, les logiciels et les abonnements) et de plus en plus aussi pour d'autres produits offerts par voie

électronique. Il existe un marché mondial en pleine expansion. Pour le consommateur qui possède une carte de crédit et qui a accès à l'Internet, l'emplacement du fournisseur n'a plus guère d'importance.

On peut également dire qu'autrefois, l'existence de barrières liées aux coûts, à la distance, à l'inaccessibilité, à l'incompatibilité et l'impossibilité de découvrir l'identité assurait parmi les meilleures protections en matière de vie privée. Les possibilités offertes par l'Internet ont tout changé. Ainsi que cela a déjà été mentionné, les FTD en ligne (de consommateur à entreprise) posent tout à la fois de nouveaux problèmes de protection de la vie privée et offrent de nouveaux moyens d'assurer cette protection. Ils facilitent la collecte de renseignements à caractère personnel qui peuvent être utilisés pour établir le profil personnel d'un usager. Il est important que la personne concernée soit informée de la collecte d'information à son sujet et de l'utilisation qui en sera faite, qu'elle ait le choix de donner ou non son consentement, et que son choix soit respecté. A cet égard, la mise en œuvre de moyens techniques peut faciliter aux personnes concernées l'exercice de leurs droits. Les profils personnels pourraient alors servir à personnaliser ou individualiser les interactions entre particuliers et entreprises.

Questions communes aux contrats interentreprises et aux contrats consommateur-entreprise

Un grand nombre de questions relatives aux contrats interentreprises sont pertinentes dans le contexte des transactions entre les consommateurs et les entreprises :

- L'information des personnes concernées quant à la collecte des données et aux finalités de cette collecte.
- La réparation des atteintes à la vie privée.
- L'existence de mécanismes de vérification efficaces.

Différences entre les contrats interentreprises et les contrats consommateur-entreprise

Il existe néanmoins entre les deux catégories de FTD d'importantes différences, qui pourraient commander l'adoption de stratégies différentes. Ainsi, dans les contrats interentreprises, il est fort probable que les deux parties seront considérées comme effectuant un traitement de données à caractère personnel auquel pourront trouver à s'appliquer des dispositions des législations nationales ou des principes d'instruments internationaux, comme les Lignes directrices de l'OCDE sur la protection de la vie privée. Souvent, le transfert de données à caractère personnel constituera la raison première, l'objectif principal de l'accord (par exemple la vente d'une liste de noms et adresses -- de plus en plus, des adresses électroniques -- à des fins de marketing direct). Lorsque le transfert effectué sera accessoire à l'objectif principal des parties, par exemple s'il s'agit d'un transfert de données personnelles concernant l'itinéraire d'un passager entre deux sociétés aériennes faisant partie d'une alliance internationale, il se déroulera le plus souvent dans le cadre d'une relation suivie entre les parties.

La situation est différente en ce qui concerne les interactions consommateur-entreprise. Souvent il n'y aura pas au départ de lien préexistant ; le consommateur aura navigué sur le Web au hasard et l'on sait que beaucoup de contacts avec les entreprises sont établis lors d'une première visite ou d'une visite occasionnelle. Exceptionnellement, le consommateur aura déjà établi une relation avec l'entreprise, par exemple lors d'une commande antérieure à une entreprise donnée ou lors d'une demande de crédit. Les parties seront également éloignées les unes des autres, dans l'espace et/ou dans le temps, mais les caractéristiques techniques du support sont conçues pour faciliter le transfert des données en dépit de ces différences. La divulgation d'information est rendue possible par l'utilisation

des logiciels d'exploration du Web qui permettent d'identifier le réseau et l'appareil utilisés pour accéder au Web, ainsi que les adresses URL des sites préalablement visités, ainsi que par le rapprochement des renseignements obtenus au moyen des témoins de connexion *(cookies)* et des données à caractère personnel. La collecte et le stockage des données sont facilités par la mise en mémoire cache et la présence de moteurs de recherche, de robots et d'index Internet.

La collecte de données la plus explicite se produit lorsque le consommateur fournit des renseignements personnels au cours d'une interaction sur un site Web, qu'il s'agisse de renseignements concernant sa carte de crédit ou d'autres modes de paiement, de ses coordonnées, ou de ses préférences personnelles. De manière générale, dans les transactions portant sur l'achat de biens ou de services, le transfert de données ne constitue pas l'objectif premier, mais est connexe à l'achat.

Ainsi que cela a déjà été mentionné, ce qui distingue principalement les transactions interentreprises des transactions consommateur-entreprise, c'est que le transfert des données entre le consommateur et l'entreprise se déroule en général sans qu'aucun contrat n'ait été conclu entre les parties. Tel est le cas, par exemple, lorsqu'une société dispose d'un site Web à partir duquel elle offre des produits et services. Par analogie avec les achats traditionnels -- pour lesquels lorsque le consommateur entre dans un magasin, aucun contrat n'existe entre lui et le commerçant --, le fait d'accéder à un site Web ne crée pas de lien contractuel entre le visiteur et le propriétaire du site, et cela en dépit du fait que des données personnelles peuvent être recueillies dès que l'usager accède au site, notamment par l'intermédiaire d'outils comme les *cookies*, qui permettent de collecter des informations et de les rattacher à une personne identifiable. Comme nous le verrons plus loin, cette particularité commande que toute mesure destinée à protéger la vie privée du consommateur soit mise en œuvre avant la formation d'un contrat.

Nécessité de diverses mesures de protection de la vie privée dans les relations consommateur-entreprise.

Si l'on considère les caractéristiques des transferts consommateur-entreprise à la lumière des règles substantielles proposées plus haut (voir section 2), il est possible de satisfaire aux exigences en matière de protection de la vie privée, même si les relations consommateur-entreprise se prêtent difficilement à l'utilisation de la structure contractuelle. Il faudrait d'autres moyens pour encourager les entreprises (importateurs de données) à adopter des mesures de protection de la vie privée. L'application d'une loi nationale dans un environnement de réseaux où les parties à un FTD en ligne ne partagent pas le même espace géographique et où les limites territoriales ont perdu leur sens se heurte à des obstacles évidents. L'application extraterritoriale de toute loi nationale sur la protection de la vie privée a en effet ses limites. Dans ces conditions, les dispositifs d'autorégulation ou les mesures efficaces prises par le secteur privé constituent des moyens importants pour réaliser les objectifs énoncés dans les Lignes directrices de l'OCDE sur la protection de la vie privée.

Pour ce qui concerne la possibilité d'élaborer une norme mondiale de protection de la vie privée, un groupe consultatif *ad hoc* agissant pour le compte de l'Organisation internationale de normalisation (ISO) a effectué une étude visant à déterminer la nécessité d'une norme internationale pour protéger la confidentialité de l'information, mesurer le degré de protection de la vie privée et assurer une harmonisation au plan mondial. Le groupe consultatif est parvenu à la conclusion qu'il était trop tôt pour déterminer s'il était souhaitable et possible que l'ISO entreprenne d'élaborer des normes internationales relatives à la protection des données à caractère personnel.

Importance des politiques types de protection de la vie privée

Il semble que les initiatives d'ordre pédagogique destinées à aider les organisations à élaborer des déclarations exactes en matière de vie privée aient un rôle important à jouer dans le contexte des transferts consommateur-entreprise. L'utilisation du générateur de déclaration de politique de protection de la vie privée élaboré par l'OCDE pour produire une déclaration de politique de vie privée (l'outil est appelé « générateur » et son résultat « déclaration »), en est un exemple. La généralisation de la pratique consistant pour les entreprises (fournisseurs/importateurs de données) à établir une politique officielle de protection de la vie privée et à diffuser cette politique dans une déclaration telle que celle produite à l'aide du générateur, pourraient avoir un effet cumulatif considérable sur la sensibilisation des consommateurs à l'égard des pratiques de traitement de l'information qui ont cours sur les sites Web et dans les entreprises en ligne avec lesquels ils entrent en relation.

Mesures de certification relatives aux transferts en ligne

L'intensification des transferts consommateur-entreprise dans le monde a comme autre conséquence de stimuler l'intérêt pour l'élaboration d'outils ou de mesures de vérification adaptés à l'environnement en ligne. Dans le cadre d'un marché mondial, où il n'existe aucune relation directe ou matérielle entre les parties lors d'une interaction sur le Web, construire la confiance des consommateurs revêt une importance primordiale. A cet égard, les efforts consacrés au développement de mesures de certification (notamment l'utilisation de labels, de sceaux et de certificats attestant du degré de protection de la vie privée) constituent des mesures volontaristes prises par le secteur privé pour gagner la confiance des consommateurs. Cette situation contraste avec d'autres mesures de protection de la vie privée qui reposent sur un processus de dépôt de plainte et sur la capacité des particuliers à faire respecter leurs droits en matière de vie privée et à intenter des poursuites. L'intérêt que suscitent les mesures de vérification montre que l'on reconnaît les obstacles juridiques et logistiques auxquels sont confrontées les personnes concernées (les consommateurs) dans le cadre des FTD consommateur-entreprise.

Recours des particuliers et respect des obligations

Il est inévitable d'évoquer les difficultés qu'éprouve le particulier à faire respecter ses droits et à exercer un recours, ainsi que la nécessité de trouver des options de règlement des litiges qui soient adaptées aux caractéristiques et aux besoins spécifiques des transferts consommateur-entreprise. Il s'agit là d'une conclusion et d'un champ d'intérêt que partagent d'autres organisations qui travaillent actuellement sur les répercussions de l'infrastructure mondiale de l'information sur les mécanismes de règlement des litiges pour les transactions commerciales électroniques ou sur le règlement des plaintes concernant l'attribution des noms de domaines. L'importance de la question du règlement des litiges, ainsi que l'existence de certaines options sont examinées dans la section 6.

Avantages pour les entreprises

Bien que l'on puisse être porté à croire que les mesures prises en faveur de la protection de la vie privée, telle l'élaboration de déclarations de politique de protection de la vie privée, servent avant tout les intérêts des consommateurs, elles peuvent aussi avoir leur utilité pour les entreprises, en particulier pour les PME. Lorsque les fournisseurs ne disposent pas d'informations suffisantes sur le commerce international, ils peuvent très bien ignorer les exigences légales qui ont cours dans d'autres juridictions

dans des domaines comme la protection des données et le marketing direct. L'utilisation de clauses types et de modèles de politiques peut leur être d'une grande utilité pour limiter les risques de plaintes (et de litiges) et contribuer à instaurer le climat de confiance qui constitue une condition préalable au succès du commerce électronique. Cependant, l'affichage d'une déclaration de politique de protection de la vie privée inexacte peut engager la responsabilité juridique de l'entreprise. C'est pourquoi celle-ci doit minutieusement examiner tout modèle de politique ou de déclaration pour s'assurer qu'elle correspond à ses pratiques en matière d'information commerciale et qu'elle est conforme à la réglementation en vigueur.

Questions soulevées par l'application de l'analyse contractuelle aux transactions consommateur-entreprise

La formation et le contenu d'un contrat sont régis par des prescriptions légales diverses, et des différences considérables existent entre les pays en ce qui concerne le droit des contrats. L'analyse qui suit vise néanmoins à relever un certain nombre d'éléments communs qui, lorsqu'on les applique dans le cadre des solutions contractuelles pour la protection de la vie privée, posent des difficultés dans les transferts consommateur-entreprise. En effet, bon nombre des interactions entre consommateurs et entreprises ne peuvent être analysées dans une perspective contractuelle ; soit qu'elles ne comportent pas les éléments d'un contrat, soit qu'elles ne satisfassent pas aux conditions préalables à la création d'un contrat.

Exigences relatives à la formation d'un contrat

En général, la doctrine de l'autonomie de la volonté permet aux parties d'établir un contrat de la façon et selon les dispositions qu'elles jugent appropriées. L'obligation que les contrats soient parafés par les parties, ou conclus d'une façon ou d'une autre par écrit, a été mise en évidence comme constituant un obstacle à l'expansion du commerce électronique. Diverses propositions ont été formulées pour remédier à cet état de choses, notamment la reconnaissance de la validité juridique des signatures électroniques ou numériques. Ces questions dépassent cependant la portée du présent rapport.

La principale exigence concernant la formation d'un contrat est la nécessité, au départ, d'une volonté de créer une pleine obligation juridique, ce dont témoigne l'offre d'une partie qui est acceptée par l'autre. Lorsque les contrats sont conclus à distance, il peut être important de déterminer à quel moment au cours du processus de commande l'accord a été conclu (c'est-à-dire à quel moment ce dernier devient irrévocable). Une fois qu'il y a accord, aucune des parties ne peut en modifier unilatéralement les conditions, bien qu'il puisse être prévu dans le contrat initial que l'entreprise peut le modifier moyennant préavis. Ces conditions peuvent avoir une importance considérable du point de vue de la protection des données. En effet, si un consommateur n'a pas été informé, au moment de la conclusion du contrat, des intentions du fournisseur quant au traitement subséquent des données personnelles le concernant, ou n'a pas donné son accord à cet effet, l'utilisation ultérieure qui est faite de ces données demeure-t-elle régie par un contrat exécutoire ? Sur quoi peut-on se fonder pour faire valoir que le fournisseur (l'entreprise) est obligé, en vertu des transactions ou actions antérieures, de protéger la vie privée du consommateur ?

Dans de nombreuses juridictions, pour qu'un contrat soit exécutoire, il faut qu'une offre ait été faite par l'une des parties et acceptée par l'autre. Il importe de déterminer à quel moment sont franchies ces deux étapes. En général, lorsqu'un fournisseur indique qu'il a des biens ou services à offrir, il ne s'agit pas d'une offre en soi, mais plutôt, selon les tribunaux des pays de *Common Law*,

d'une invitation lancée aux consommateurs pour qu'ils fassent une offre, laquelle peut ensuite être acceptée par le fournisseur. Il y a alors formation de contrat. Le moment précis de la formation du contrat dépendra des règles d'acceptation applicables.

Les règles d'acceptation sont actuellement à l'étude dans les pays qui veulent moderniser leur législation et assurer une plus grande sécurité quant à son application dans le cyberespace. A titre d'exemple, selon le projet de directive de l'UE sur le commerce électronique, le fournisseur peut être réputé avoir fait l'offre, mais :

> *« Les États membres prévoient dans leur législation que, sauf si les parties sont des professionnels et en sont convenues autrement, dans le cas où le destinataire du service est requis, lors de l'acceptation de l'offre du prestataire, d'exprimer son consentement en utilisant des moyens technologiques, tels que cliquer sur une icône, le contrat est conclu au moment où le destinataire du service reçoit, par voie électronique, du prestataire de service, l'accusé de réception de l'acceptation du destinataire du service » (article 11).*

Cet accusé de réception, qui doit être envoyé immédiatement, est réputé reçu au moment où il devient accessible au consommateur, ce qui ne correspond pas nécessairement au moment où ce dernier en prend connaissance. Il peut suffire qu'il soit livré dans la boîte aux lettres électronique du consommateur. C'est là un autre aspect contractuel actuellement à l'étude.

La Chambre de commerce internationale (CCI) travaille également sur l'établissement de règles uniformes pour le règlement des échanges électroniques. Ces règles adoptent une approche différente, car elles stipulent que :

> *« Une offre et/ou une acceptation faite par voie électronique est effective lorsqu'elle entre dans le système d'information du bénéficiaire sous une forme que ce système peut traiter ou lire. » (Règle 2.1)*

Aux États-Unis, le *Uniform Computer Information Transactions Act* stipule ce qui suit :

> *« ARTICLE 203. OFFRE ET ACCEPTATION - PRINCIPES GENERAUX. A moins que les circonstances ou les termes ne l'indiquent autrement et sans équivoque :*
>
> *(1) Une offre de conclure un contrat est une invitation qui peut être acceptée sous quelque forme et par quelque moyen raisonnable que ce soit selon les circonstances.*
> *(2) Toute commande ou offre d'acquérir une copie destinée à être livrée rapidement ou incessamment appelle une acceptation, soit par la promesse rapide d'expédition, soit par l'envoi rapide ou immédiat d'une copie conforme ou non conforme. Cependant, l'envoi de copies non conformes ne constitue pas une acceptation si le concédant avise de façon raisonnable le cessionnaire que l'envoi est offert uniquement par esprit de conciliation à l'égard de ce dernier.*
> *(3) Si le début de la réalisation demandée constitue un mode d'acceptation raisonnable, l'offrant qui n'est pas avisé de l'acceptation dans un délai raisonnable peut conclure que l'offre a pris fin avant qu'elle n'ait été acceptée.*
> *(4) Si une offre présentée dans un message électronique appelle une réponse par message électronique, un contrat est formé :*
>
> *(A) Lorsque l'acceptation électronique est reçue ; ou,*

(B) Si la réponse est constituée par le début de la réalisation, l'intégralité de la réalisation, ou l'accès à des informations, lorsque la réalisation est reçue ou l'accès permis et que les éléments nécessaires à l'accès ont été reçus. »

D'autres circonstances influent sur l'analyse contractuelle appliquée aux FTD. Certaines compliquent la situation, telle l'utilisation par le consommateur d'une carte de crédit pour régler la transaction et la nécessité de fournir à l'avance les détails s'y rattachant. Les renseignements concernant la carte de crédit peuvent être facilement traités et vérifiés par le fournisseur avant que le consommateur ne soit informé de l'acceptation de sa commande. Lorsque le fournisseur a effectivement accepté l'argent du consommateur, il peut devenir difficile de contester la formation d'un contrat.

Si le contenu des déclarations en matière de politique de protection de la vie privée devait être intégré dans des contrats entre entreprise et consommateur, il conviendrait que soit clairement précisée la version de la déclaration qui s'applique à chaque contrat. Des aménagements d'ordre technique ou de procédure devraient être mis au point pour garantir la sécurité juridique de contrats avec les consommateurs basés sur le contenu de pages Web et autres documents de même nature proposés sur les réseaux mondiaux.

Harmonisation des différentes approches concernant les contrats en ligne

Ces exemples montrent que les conditions nécessaires à la formation d'un contrat dans un environnement en ligne ne sont pas encore fixées. Toutefois, diverses approches sont actuellement préconisées et des efforts importants sont déployés à l'échelle internationale pour les unifier. Cette démarche revêt une grande importance pour l'application des structures contractuelles aux interactions consommateur-entreprise sur le Web. En effet, l'internaute qui visite un site Web peut, du seul fait de sa présence sur le site, générer des données le concernant, et ceci constitue une forme de transfert de données qui, de surcroît, pourrait être aussi de type transfrontières. Dans un tel cas, le particulier n'a pas encore passé de commande de produits ou services, mais seulement visionné le site ou téléchargé de l'information ; il s'est contenté de faire du « lèche écran » et il est peu probable que les obligations contractuelles liées à l'intention de s'engager ou à une offre et son acceptation puissent s'appliquer à ce qui par essence constitue une simple communication ou interaction.

Pour ceux des transferts consommateur-entreprise qui sont structurés de façon à former un contrat, le résultat des diverses initiatives relatives aux obligations contractuelles dans le cadre des transactions commerciales électroniques pourra s'appliquer directement aux contrats consommateur-entreprise relatifs à la protection de la vie privée en ligne. Parmi ces initiatives, mentionnons la reconnaissance juridique des mesures d'authentification (telle que l'utilisation de la signature numérique ou électronique) et la rationalisation des obligations en matière de preuve. Des travaux sont également en cours pour résoudre les conflits de lois (choix du droit applicable et de la compétence juridictionnelle) dans les transactions transfrontières.

Utilisation de l'Internet pour l'enregistrement de la formation d'un contrat

Les capacités de stockage et d'enregistrement de l'information qu'offre l'Internet présentent un avantage. Contrairement à la grande majorité des contrats matériels, qui peuvent être conclus de façon non officielle, sans vraiment qu'aucune preuve n'atteste de leur contenu et encore moins des conditions qui les régissent, l'utilisation d'Internet permet de tenir un registre complet de chaque action qui a eu lieu lors de la formation et de la conclusion d'un contrat. Si l'enregistrement de ces

données peut constituer en soi un motif de préoccupation concernant la protection de la vie privée, il peut néanmoins être utile pour reconstituer toutes les étapes du processus de création du contrat si cela devenait nécessaire.

Possibilités offertes par les politiques de protection de la vie privée dans les transferts consommateur-entreprise

Les politiques et déclarations en matière de protection de la vie privée sont un moyen de notifier les personnes physiques. Ces notifications sont susceptibles de créer des obligations contractuelles et d'autres obligations légales telles que des responsabilités statutaires ou réglementaires. L'exécution de ces obligations peut, selon la nature de la responsabilité et du droit applicable, être poursuivie par les parties au contrat, les diverses personnes concernées ou par des organismes publics.

Nécessité de présenter dès le début de l'interaction une mise en garde au sujet de la vie privée

Pour offrir une véritable liberté de choix au consommateur quant aux transferts des données le concernant, il ne suffit pas de l'informer de l'usage qui pourrait être fait de ces données au moment de la conclusion d'un contrat de fourniture de biens ou de services. Bien davantage, il importe de soumettre à son attention les questions relatives à la protection de la vie privée le plus tôt possible lors de sa visite sur le site.

Il serait tout à fait possible qu'un site adopte une politique de protection de la vie privée et la fasse connaître. Le particulier serait ainsi informé de la nature des données qui seraient recueillies sur lui et des utilisations subséquentes que l'on pourrait en faire.

Mise en œuvre des déclarations de protection de la vie privée

L'incorporation des dispositions relatives à la protection de la vie privée dans un contrat entre un consommateur et une entreprise permettrait au consommateur d'engager une action pour les faire respecter. Toutefois, dans certaines juridictions, le statut juridique des politiques ou déclarations de protection de la vie privée n'est pas clair et les moyens dont dispose le consommateur pour les faire respecter sont parfois limités. Quoi qu'il en soit, tout consommateur qui voudrait intenter une poursuite contre une entreprise exerçant ses activités sur le Web doit surmonter des obstacles concrets, compte tenu des ressources nécessaires à un tel recours. L'une des difficultés est de déterminer quel tribunal est compétent pour entendre la cause, à supposer qu'il soit possible d'établir l'emplacement géographique de l'entité responsable du contenu du site Web ou des pratiques en matière d'utilisation et de divulgation des renseignements personnels associées à ce site. Autant de raisons en faveur du développement de mécanismes de règlement des litiges auxquels les entreprises comme les consommateurs pourraient avoir facilement accès, qui seraient crédibles et bien acceptés par les milieux d'affaires. Il conviendrait en particulier que les procédures de traitement des plaintes et de règlement des litiges en ligne soient conçues de telle façon que les entreprises, les concepteurs de sites Web et les fournisseurs de services Internet (FSI) qui effectuent des transferts de données en ligne soient convaincus de l'intérêt qu'ils ont à les mettre en œuvre et à les respecter.

Aux États-Unis, la *Federal Trade Commission* est habilitée, en vertu de l'article 5 de sa loi constitutive, qui interdit les pratiques ou actes trompeurs ou déloyaux, à intenter des actions en justice contre des organisations qui se livrent à de tels actes ou pratiques dès lors qu'ils s'inscrivent dans l'exercice d'activités commerciales ou ayant une incidence sur le commerce. La FTC a déclaré que la

représentation matérielle erronée de la finalité en vue de laquelle une information est recueillie auprès des consommateurs, ou de l'usage qui sera fait de cette information, constitue une pratique trompeuse. Entrerait dans la catégorie des pratiques ou actes déloyaux ou trompeurs le fait, pour une organisation, de déclarer adhérer à la politique de protection de la vie privée qu'elle affiche sur son site, alors qu'il n'en est rien.

Les exigences en matière de preuve, de sécurité et d'authentification d'un contrat de protection de la vie privée ayant force obligatoire ne seraient pas différentes de celles qui ont été discutées pour les contrats interentreprises dans le cadre du commerce électronique. La solution apportée à ces questions (dans le contexte du commerce électronique) devrait également être appliquée aux contrats de protection de la vie privée entre un consommateur et une entreprise.

Nécessité de mécanismes de vérification

La vérification (qu'elle prenne la forme d'une autoévaluation, d'un certificat, d'un label ou autre) revêt une très grande importance dans les transactions entre consommateurs et entreprises. Le consommateur doit avoir confiance dans les pratiques suivies en matière d'information par un site Internet dont il ne connaît pas l'emplacement et dont l'identité des responsables -- personnes ou entreprise -- pourrait être impossible à déterminer. Étant donné que les possibilités de négociation des conditions d'un contrat entre consommateur et entreprise sont limitées, la participation d'un tiers peut s'avérer souhaitable pour confirmer que le contrat satisfait aux normes de protection de la vie privée et que le site ou l'entreprise s'acquitte de ses obligations dans ce domaine. La même suggestion vaut pour les déclarations de politique de protection de la vie privée.

Options de vérification électronique

Le besoin d'un mécanisme quelconque de vérification a déjà été abordé dans le cadre de la discussion sur les contrats interentreprises. Les clauses modèles de la CCI prévoient une gamme d'options pour l'inspection ou la vérification par un tiers de l'exécution des obligations d'un importateur de données en matière de protection de la vie privée. Dans le contexte des transactions consommateur-entreprise, cette question est davantage apparue comme relevant de la protection du consommateur. C'est aux caractéristiques de l'environnement en ligne, dans lequel les données sont souvent recueillies par l'entremise d'un site Web, que l'on doit un intérêt précoce pour l'utilisation de marques, de labels ou de sceaux attestant de la protection de la vie privée plutôt que pour l'inspection ou la vérification physique, qui présuppose une visite des lieux. De nombreuses initiatives internationales ont été prises pour développer des mesures de vérification pour l'Internet. Quelques-unes d'entre elles sont décrites ci-dessous.

Le sceau délivré par *Better Business Bureau Online*, le site Web TRUSTe et la marque de certification du Japon visent à accroître la protection de la vie privée dans un cyberespace mondial. Ces instruments pourraient également s'appliquer au traitement transfrontières de données à caractère personnel. Les sites Internet produisant toujours des flux transfrontières de données, les sites Internet américains qui affichent les sceaux BBB Online ou TRUSTe s'attachent à renforcer la protection de la vie privée dans l'environnement électronique mondial. Ils reposent sur des systèmes d'autorégulation dus à l'initiative du secteur privé aux États-Unis.

Il existe au Japon deux systèmes d'attestation de protection de la vie privée : le *Japanese Privacy Protection Mark System* et le *Granting Mark System.* Le premier est exploité depuis avril 1998 par le Centre japonais pour le développement du traitement de l'information (JIPDEC), et le second par

l'Association japonaise de transmission de données. Le JIPDEC délivre les marques de certification au terme d'un processus visant à vérifier que le traitement des données à caractère personnel est conforme aux lignes directrices de 1997 du ministère de la Technologie de l'Information et de l'Industrie (MITI). De son côté, l'Association japonaise de transmission de données délivre les marques de certification aux opérateurs de télécommunications et aux fournisseurs de services, après s'être assurée de leur conformité aux lignes directrices de 1996 et de 1998 du ministère des Postes et des télécommunications (MPT).

Rôle des technologies de protection de la vie privée

Le *World Wide Web Consortium* (W3C) a lancé le projet *Platform for Privacy Preferences* (P3P), qui a pour but de faciliter, dans un cadre souple, un accord contractuel entre fournisseurs d'information et utilisateurs du Web qui permette au fournisseur de tenir compte des préférences d'un utilisateur en matière de protection de la vie privée. Les principaux fabricants de logiciels ont annoncé qu'ils incorporeront la P3P dans leur prochaine version de logiciel, lorsqu'elle sera ratifiée par le W3C.

Le P3P repose sur certaines conditions techniques qui ne sont pas encore toutes réunies. Les logiciels de navigation des utilisateurs et les fournisseurs devront être compatibles pour permettre la négociation entre les ordinateurs personnels et les serveurs. Les préférences peuvent être différentes selon les régions du monde, par exemple dans l'UE et aux États-Unis par rapport aux pays arabes ou asiatiques, ce qui pose des problèmes de compatibilité.

Un autre exemple qui pourrait servir de point de départ est le *Merchant Server* de Microsoft qui est utilisé pour lancer une opération de commerce électronique. Des détaillants de secteurs très variés y ont recours. L'avantage de cette fonction normalisée est de fournir l'occasion d'intégrer des politiques de protection de la vie privée dans la conception du logiciel. Toutefois, à l'heure actuelle, la seule dimension de la protection de la vie privée qui est prise en compte concerne la sécurité des échanges de données financières avec les logiciels cryptographiques. Davantage d'attention pourrait être portée à la possibilité de collaborer avec les principaux concepteurs et fournisseurs de logiciels pour que la protection de la vie privée soit prise en compte à toutes les étapes de la conception, de la production et de l'utilisation d'un logiciel.

Initiatives concernant la protection du consommateur

Plusieurs acteurs, gouvernementaux ou non gouvernementaux, pourraient jouer un rôle dans la protection du consommateur en ligne, notamment dans la protection de sa vie privée. Tel est le cas, par exemple, aux États-Unis, des *Better Business Bureaux,* qui sont chargés de protéger les intérêts des consommateurs.

Le *Better Business Bureau Online* (BBB Online), TRUSTe et WebTrust ont conçu et développé des dispositifs de vérification par des tiers qui favorisent le respect de codes de bonne conduite en matière d'information. Ces dispositifs reposent sur l'affichage d'un sceau ou d'une marque dite « de confiance » indiquant aux consommateurs que les sites Web se conforment à des pratiques loyales en matière d'information. Tous ces organismes proposent des mécanismes de règlement des litiges, contrôlent le respect des engagements pris et agissent en cas de non-conformité (sanctions ou expulsion du site fautif du programme de label de confiance). Les entreprises qui enfreignent les pratiques qu'elles ont déclaré suivre en matière d'information s'exposent également à des actions de la FTC en vertu de l'article 5 de la loi relative à la FTC.

Ces organismes peuvent avoir un impact sur les discussions, même s'ils sont parfois eux-mêmes actifs sur la scène commerciale. Par exemple, au Royaume-Uni, l'Association des consommateurs (*Consumers Association*) vend des livres et des revues, émet sa propre carte de crédit et agit en qualité de fournisseur de services Internet.

Dans certains cas, par exemple le *Web Trader Scheme* exploité par l'Association des consommateurs du Royaume-Uni, les commerçants agréés sont autorisés à s'identifier comme tels sur leur site Internet au moyen d'un label. Les entreprises agréées sont tenues de respecter un code de conduite qui comprend l'obligation de se conformer à la loi de 1998 sur la protection des données. L'Association des consommateurs s'engage à garantir, à hauteur de GBP 50, les pertes financières causées par l'emploi abusif des données relatives à une carte de crédit transmises à un commerçant agréé. L'Association n'assume pas de responsabilité concernant d'autres pertes, y compris celles qui seraient la conséquence d'une violation de la loi sur la protection des données.

L'existence d'une entité fédératrice des entreprises pourrait permettre d'incorporer la protection de la vie privée dans les conditions préalables à l'inscription sur un site Internet. Tel est le cas, par exemple de Bizrate, un organisme situé à Los Angeles qui exploite un site Internet répertoriant les entreprises dans des catégories très diverses. Pour être inscrite dans le répertoire, l'entreprise doit accepter une évaluation par le personnel de l'organisme ou par ses clients. Dans les deux cas, l'évaluation est menée selon une grande variété de critères, y compris la politique de protection de la vie privée affichée par le commerçant. Les programmes de certification et de labellisation peuvent se révéler très utiles pour renforcer d'autres mesures de protection de la vie privée telles que l'utilisation de déclarations de politique en ce domaine. Lorsque le consommateur et l'entreprise sont situés dans des pays différents, il peut être extrêmement difficile pour le consommateur de faire valoir ses droits contre l'entreprise. L'intégration de mécanismes alternatifs de règlement des litiges à ces initiatives constituerait un précieux complément à la protection juridique des consommateurs. C'est ce qui sera examiné dans la section suivante.

Faire respecter les engagements en matière de protection de la vie privée dans les transactions entre consommateurs et entreprises

Les droits du consommateur en matière de protection de la vie privée sont stipulés dans des lois nationales et peuvent être exercés selon les conditions qu'elles prescrivent. La plupart des régimes de protection des données englobent les données et supports de traitement électroniques, de sorte que si l'activité en ligne entre dans le champ d'application d'une loi nationale, le consommateur doit être en mesure de s'adresser à l'autorité compétente pour obtenir réparation.

Validité des droits contractuels

Quand une entreprise déclare son adhésion à une politique de protection de la vie privée, le respect de cette déclaration est susceptible de faire partie des conditions de tout contrat conclu avec un consommateur. Le contrat conclu entre un consommateur et une entreprise présente un avantage par rapport au contrat interentreprises car la personne concernée par le recueil de données est en principe une des parties contractantes ; la non reconnaissance de la stipulation pour autrui serait donc sans effet. En cas de non-respect, plusieurs voies de recours sont possibles, bien que leur efficacité ne soit pas assurée dans le contexte de l'Internet. En théorie, toute entreprise qui ne respecte pas un engagement contractuel à ne pas divulguer des données à caractère personnel à des tiers pourrait être poursuivie par le consommateur. Mais même si une action était engagée contre une entreprise pour prévenir des violations ultérieures, elle ne pourrait annuler un transfert de données déjà produit, et les réparations

que le consommateur pourrait obtenir auraient les mêmes limites que celles qui ont déjà été évoquées dans le cadre de l'examen des actions en justice concernant les contrats interentreprises.

Dans les cas où aucun contrat n'est formé entre le consommateur et l'entreprise (par exemple, l'information sur le consommateur a été obtenue lorsque celui-ci a visité le site, mais sans qu'il en résulte un contrat), il est possible que l'entreprise se trouve en situation de manquement à ses obligations contractuelles à l'égard du tiers qui a certifié la politique de protection de la vie privée ou qui a permis l'utilisation d'un label recommandant le site en cause. Dans le passé, de telles situations ont soulevé des inquiétudes dans les pays de *common law*, en vertu duquel les droits et les recours stipulés dans un contrat ne lient que les parties contractantes. Cependant, comme cela a déjà été noté, la question de la connexité contractuelle a été résolue par plusieurs pays, qui ont adopté des lois spécifiques pour reconnaître les droits des tiers bénéficiaires. Toutefois, la question de l'efficacité des recours actuels reste entière.

Autres recours et réparation de nature civile

L'éventail des recours de nature civile que peut exercer une personne concernée par le traitement de ses données n'est pas limité à ceux qui sont prévus par les lois de protection de la vie privée. D'autres lois sur la protection du consommateur peuvent s'appliquer, telles celles qui interdisent la publicité mensongère ou de nature à induire en erreur (voir l'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). Les lois générales relatives à la non-exécution des contrats, à la fraude et aux pratiques commerciales déloyales peuvent également s'appliquer lorsque le responsable des traitements n'a pas respecté les termes et conditions de sa déclaration de protection de la vie privée, ou un accord en ligne (par exemple, les conditions qui régissent les formulaires d'inscription) ou un contrat de flux transfrontières de données. Une telle violation peut donner lieu à diverses réparations de nature civile. Essentiellement, lorsqu'un site Web affiche ses pratiques en matière de protection de la vie privée, il signifie qu'il s'engage à respecter ces pratiques. Si cet engagement n'est pas tenu, et selon la nature de la violation, il est possible, dans la plupart des juridictions d'exercer un recours dans le cadre des lois sur la protection du consommateur et sur les pratiques commerciales, pour déclaration mensongère et/ou fraude.

Droit applicable et compétence juridictionnelle

Définir la territorialité selon un critère géographique

Un transfert consommateur-entreprise peut faire intervenir de nombreux participants (ou acteurs). Il serait réducteur de parler seulement de consommateurs et d'entreprises. L'Internet compte en effet de nombreux intermédiaires qu'il s'agisse des fournisseurs de services, ou de l'enchaînement des technologies sur lesquelles le réseau repose (utilisation de serveurs pour accueillir les pages Web et les fichiers, réacheminement des paquets de données par des nœuds partout dans le monde, et mise en mémoire cache). Chacun de ces acteurs (y compris le responsable du traitement) et chacune de ces activités peut relever des différents territoires juridiques. Le plus souvent, les participants à un transfert consommateur-entreprise ne se connaissent pas (dans le cadre d'une relation préexistante ils ne seront pas considérés comme expéditeur et destinataire). La question qui se pose est de savoir quelle est la règle de droit national applicable au transfert de données, au contenu des messages ou à d'autres activités auxquelles l'Internet permet d'avoir accès ? Quels sont les tribunaux compétents pour trancher des litiges civils et engager des poursuites en cas de violation ? La présomption de lieu

physique et de proximité (qui est inhérente au lien entre territorialité et frontières géographiques) est remise en question dans ses fondements mêmes par les caractéristiques des réseaux mondiaux.

Choix du droit applicable et de la compétence juridictionnelle

Le choix du droit applicable revêtira une importance déterminante pour l'adaptation et la mise en œuvre des solutions contractuelles en matière de protection de la vie privée. Bien qu'un tribunal puisse avoir compétence *ratione personae*, le choix des règles de droit pourrait conduire à ce que le litige doive être traité selon la législation d'un autre état. Chaque pays a son propre droit international privé (qui fait partie de son droit interne ou national). Malgré les différences, de nombreux efforts sont consentis pour harmoniser les règles de conflits des lois. De nombreuses juridictions ont des objectifs communs et sont sensibles au principe de courtoisie et au besoin de respecter les systèmes de justice civile des autres pays.

La question de savoir où et quand un contrat est conclu est importante pour déterminer le droit qui régira cette transaction. Comme cela a été souligné, lorsque les transactions ont lieu sur l'Internet, il n'est pas toujours facile de répondre à cette question. Le nom de domaine mondial de premier niveau .COM ne donne aucune indication sur l'emplacement d'une entreprise. Même lorsque le nom utilise un code de pays comme .DE ou .UK, rien ne garantit que l'entreprise soit située dans ce pays. En effet, deux caractéristiques fondamentales de l'Internet sont sa capacité de réacheminement et son anonymat.

En général, les parties contractantes sont libres de choisir le système juridique qui régira une transaction, sous réserve que ce choix revête un caractère raisonnable. A cela s'ajoute la question de savoir quel sera le tribunal national compétent pour se prononcer sur l'interprétation du contrat. A titre d'illustration, des parties résidant dans des pays différents, par exemple le Canada et l'Allemagne, seraient ainsi libres de déterminer que le contrat sera régi par le droit canadien mais que les éventuels litiges seront portés devant un tribunal allemand.

Droits des consommateurs

En Europe, les Conventions de Bruxelles et de Rome[9] prévoient des exceptions partielles dans le cas des contrats passés avec des consommateurs. Selon la Convention de Rome, un fournisseur qui a une succursale, une agence ou un établissement dans le pays de résidence du consommateur est réputé y être domicilié. Les consommateurs peuvent choisir d'intenter une poursuite soit dans leur pays de résidence, soit dans celui du fournisseur, tandis qu'une poursuite contre un consommateur ne peut être intentée que dans le pays de résidence de celui-ci.

La question de savoir si une entreprise exerçant ses activités sur l'Internet peut être réputée avoir une succursale, une agence ou un établissement dans chacun des pays à partir desquels il est possible d'accéder à son site n'est pas tranchée. L'OCDE a fait remarquer, dans le contexte des travaux sur l'harmonisation fiscale, que la notion d'établissement stable, dont l'importance est primordiale pour déterminer si une entreprise doit payer des impôts nationaux, n'est pas nécessairement pertinente dans le contexte du commerce électronique.

La Convention de Bruxelles, qui s'appuie sur les dispositions de la Convention de Rome, prévoit qu'un contrat international ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle. La portée de ces dispositions impératives n'est pas nettement définie, mais compte tenu de la dimension

« droits de l'homme » qu'attachent à la protection des données plusieurs instruments nationaux, aux droits de la personne, il est possible de soutenir que tout contrat comportant des clauses qui priveraient les consommateurs de droits qui leur sont reconnus par la Convention du Conseil de l'Europe et la directive de l'Union européenne serait déclaré inopérant sur ce fondement.

Aux États-Unis, la compétence juridictionnelle s'appuie généralement sur trois critères : i*)* le fait que l'entreprise se soit établie volontairement dans l'État du for *ii)* l'existence d'un lien de causalité entre les poursuites engagées et les activités du défendeur dans l'État du for *iii)* l'existence d'un lien juridique suffisant entre les actes du défendeur et l'État du for pour rendre raisonnable l'exercice de la compétence juridictionnelle.

Évolution récente du commerce électronique

L'évolution récente du commerce électronique est de nature à compliquer les choses. L'Union européenne a récemment publié une Directive sur le commerce électronique stipulant que, du moins dans l'Union européenne, les transactions conclues par voie électronique seront régies par le droit du pays du fournisseur. L'argument invoqué pour justifier cette approche est qu'elle favorisera l'essor du commerce électronique. Toutefois, en même temps, la Commission propose des modifications aux Conventions de Bruxelles et de Rome qui auraient pour effet d'assujettir tous les contrats conclus avec les consommateurs au droit du pays où ceux-ci ont leur résidence habituelle.

Certains considèrent qu'il y une opposition inévitable entre les dispositions relatives au choix du droit applicable et à la compétence juridictionnelle qui ont pour objet soit d'offrir un environnement prévisible aux fournisseurs, soit d'aider les consommateurs à obtenir réparation. Les mécanismes alternatifs de règlement des litiges pourraient être le moyen le plus efficace pour résoudre cette question. A cet égard, les Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique de 1999 recommande l'utilisation et la mise au point de mécanismes alternatifs de règlement des litiges, pour traiter les réclamations des consommateurs et résoudre les litiges suscités par le commerce électronique entre entreprises et consommateurs, en prêtant une attention particulière aux transactions transfrontières. Il existe un lien évident entre la protection de la vie privée et le commerce électronique. La quantité et la nature des transferts de données qui se produisent dans le commerce électronique suscitent des inquiétudes quant à la protection de la vie privée. Le manque de confiance des consommateurs dans le niveau de protection des données à caractère personnel sur l'Internet est un facteur qui entrave la croissance du commerce électronique : si la protection de la vie privée (et la capacité des personnes concernées d'obtenir réparation) trouve sa source dans les conventions sur les droits de la personne, c'est également une question qui entre dans le domaine de la protection du consommateur et il convient de concilier ces deux aspects. La question du degré d'autonomie à accorder aux parties contractantes pour déterminer le choix du droit applicable et de la compétence juridictionnelle deviendra donc une question fondamentale.

Conclusions sur les transferts consommateur-entreprise

Il faut prendre des mesures pour protéger la vie privée des consommateurs sur l'Internet en se fondant sur les Lignes directrices de l'OCDE sur la protection de la vie privée. Il n'existe pas de solution unique pour réglementer les transferts de données consommateurs-entreprises. Il existe des mécanismes de nature à aider les consommateurs à faire des choix éclairés à l'égard de la collecte et de l'utilisation de leurs données personnelles avant la conclusion de tout contrat.

Les politiques de protection de la vie privée qui s'expriment par l'affichage d'une déclaration ont un rôle primordial à jouer. Des outils comme le générateur de l'OCDE peuvent aider les entreprises à formuler une déclaration de politique ayant valeur d'engagement exécutoire. Un rôle important revient également aux organismes de protection du consommateur et aux organismes tiers dans la mise à disposition d'outils et de services de certification ou de vérification. Ces organismes pourraient même surveiller la mise en œuvre et la mise à jour des politiques des entreprises engagées dans un tel arrangement ou soumises à un organisme sectoriel ou professionnel ou à un code de conduite.

Il conviendrait dans de nombreux cas de privilégier les mesures axées sur la prévention et l'éducation telles les déclarations de politique de protection de la vie privée et les mesures de vérification. Même si les déclarations s'avèrent sans valeur contractuelle, elles restent utiles pour sensibiliser les personnes concernées et les responsables de traitements.

Toutefois, la réflexion ne doit pas porter uniquement sur la sensibilisation. Il y a lieu de se pencher également sur l'intérêt qui s'attache à prescrire à l'avance les options de règlement des litiges qui peuvent s'appliquer. Il serait peut-être possible d'adapter les projets existants de règlement des litiges en ligne pour fournir un service sur mesure destiné à constituer un premier palier de règlement des litiges relatifs à la protection de la vie privée, notamment pour « les contentieux de masse » et concernant des personnes qui ne disposent pas des ressources suffisantes pour exercer leurs autres voies de recours judiciaires.

V. Nécessité d'établir des mécanismes appropriés de règlement des litiges

L'existence de mécanismes de règlement des litiges relatifs aux FTD entre les responsables de traitements (les entreprises) et les personnes dont les données sont recueillies (les consommateurs) a été reconnue par plusieurs gouvernements de pays membres comme une exigence fondamentale. Il existe de nombreux mécanismes traditionnels et alternatifs de règlement des litiges. La présente section inclut une présentation : des avantages et inconvénients de chacun de ces mécanismes, compte tenu des spécificités de l'environnement en ligne mises en évidence par certains observateurs ; de certaines évolutions au plan international concernant le règlement des litiges en ligne, ainsi que de projets intéressants pour la création de mécanismes de règlement. Enfin, pour nourrir la réflexion, la dernière partie de la section propose quelques suggestions pour l'élaboration de mécanismes de règlement en ligne des litiges entre consommateurs et entreprises relatifs au respect de la vie privée.

Éventail des mécanismes de règlement des litiges

Lorsque survient un litige, les possibilités de recours des parties revêtent une importance cruciale. Les avantages et les inconvénients des diverses options et de leur application sont examinés ci-après. Les travaux sur les mécanismes alternatifs de règlement des litiges dans l'environnement en ligne n'en sont encore qu'à un stade tout à fait préliminaire. Dans l'analyse des options pour régler les litiges consommateur-entreprise, les caractéristiques du mécanisme de règlement sont importantes et l'on s'attachera ici à contribuer de façon préliminaire à dégager un certain nombre d'éléments clés à prendre en compte dans la conception de mécanismes visant à résoudre les différends entre consommateurs et entreprises.

Action en justice

Le recours au tribunal est toujours possible, principalement dans les litiges entre entreprises. Les parties peuvent convenir au préalable que le règlement de leurs litiges sera régi par tel droit substantiel et relèvera de telle juridiction. En revanche, si les parties ne se sont pas entendues au préalable, l'une d'elle peut, après que le litige est survenu, intenter une poursuite devant un tribunal particulier. Les parties peuvent choisir la juridiction dans laquelle le contrat a été établi, celle où est exécuté le contrat, ou toute autre juridiction ayant un lien avec l'objet du contrat. S'il s'agit d'une transaction interentreprises, il est très probable qu'un tel accord sera considéré comme valide par les tribunaux compétents.

La situation est différente lorsqu'il s'agit d'une transaction consommateur-entreprise. L'entreprise peut prévoir une clause type de règlement stipulant que tous les litiges doivent être portés devant la juridiction de son choix. Cependant, les autorités législatives hésitent souvent à imposer une clause attributive de compétence à un consommateur, qui en principe dispose de moyens plus limités que l'entreprise. De nombreux tribunaux ont ainsi annulé la clause qui contraignait le consommateur à intenter une poursuite dans la juridiction de l'entreprise. Rien ne garantit donc que les tribunaux d'une juridiction donnée valideront une telle clause.

Les avantages de l'action en justice

Il peut arriver que l'une des parties préfère régler le litige dans une juridiction qui lui est connue et où elle a déjà fait expérience du droit et de la procédure applicables. A moins que les deux parties n'aient avantage à porter l'affaire devant une juridiction particulière, d'une manière générale seule la partie jouissant d'un plus grand pouvoir contractuel sera en mesure d'imposer un tel accord préalable.

Lorsque le tribunal rend sa décision, il établit un précédent. Pour éclaircir un point de droit, il peut être avantageux d'intenter un recours en justice afin d'obtenir une décision définitive sur la question. Les autres formes de règlement n'établissent habituellement pas de précédent qui puisse servir ultérieurement. En outre, la décision définitive rendue au terme de la poursuite en justice est exécutoire et peut donc être appliquée contre la partie perdante. Dans la plupart des juridictions, la partie perdante a un droit d'appel contre une décision qui lui est défavorable. Ce droit d'appel n'existe habituellement pas dans la plupart des autres formes de règlement des litiges.

Inconvénients de l'action en justice

L'action en justice présente aussi des inconvénients. Premièrement, la procédure peut être longue : elle dure parfois des années. Deuxièmement, elle coûte très cher. Troisièmement, la partie perdante bénéficie souvent d'un droit d'appel, ce qui peut augmenter les coûts et allonger la durée de la procédure. Quatrièmement, dans la plupart des cas, la poursuite en justice n'est pas une procédure confidentielle. Lorsqu'une cause est particulièrement délicate, le caractère public de la poursuite peut avoir un effet dissuasif sur le demandeur. De surcroît dans les situations transfrontières, la partie gagnante peut se voir néanmoins obligée de s'adresser à la juridiction de la partie perdante pour obtenir l'exécution du jugement.

Résolution extrajudiciaire des conflits

Les parties à un contrat transfrontière peuvent convenir de soumettre leurs litiges à des mécanismes alternatifs de règlement. Ces mécanismes peuvent être adaptés afin que les parties bénéficient d'un maximum de souplesse. Bon nombre de ces mécanismes sont consensuels, plutôt que contentieux. Ils permettent d'éviter certains inconvénients associés à l'action en justice et à l'arbitrage : ils sont moins coûteux, aboutissent plus rapidement, offrent une perspective plus large et permettent aux parties de mieux maîtriser le processus et le résultat. Certaines des options disponibles concernant ces mécanismes alternatifs sont exposées ci-après.

Arbitrage

Tout comme pour la poursuite en justice, l'arbitrage se termine par une décision finale exécutoire à l'encontre de la partie perdante. Dans un arbitrage *ad hoc*, les parties s'entendent pour recourir à l'arbitrage, mais elles ne choisissent pas parmi les nombreuses institutions d'arbitrage celle qui arbitrera leur différent. L'arbitrage *ad hoc* est parfois moins coûteux que l'arbitrage institutionnel, mais les parties doivent se charger des tâches normalement assumées par le personnel des diverses institutions.

En arbitrage institutionnel, les parties soumettent leur litige à l'une des nombreuses institutions d'arbitrage reconnues, comme la Chambre de commerce internationale (CCI), l'*American Arbitration Association* (AAA), l'Organisation mondiale de la propriété intellectuelle (OMPI) ou la Cour d'arbitrage international de Londres (LCAI). Les parties peuvent insérer une clause dans leur contrat initial indiquant que leurs litiges seront soumis à l'arbitrage, ou s'entendre sur ce point après qu'un litige particulier se sera produit. Si elles acceptent de soumettre leur litige à l'arbitrage institutionnel, elles doivent se conformer aux règlements et procédures établis par les institutions compétentes. A moins que les parties n'y consentent, elles ne sont pas liées par les règles judiciaires de procédure et de preuve. Par conséquent, elles bénéficient souvent d'une plus grande souplesse que lors d'une poursuite en justice.

Avantages de l'arbitrage

L'arbitrage a certains avantages : les parties sont libres de choisir leurs arbitres respectifs, de même que les lois et la procédure qui régiront l'arbitrage ; une partie peut demander un arbitre ayant des compétences dans un domaine particulier et les parties peuvent éviter de porter leur cause devant le tribunal de l'un ou l'autre d'entre elles. Généralement, l'arbitrage est une voie moins coûteuse et plus rapide que l'action en justice. Les parties peuvent s'entendre pour réduire les délais, ce qui permet d'accélérer l'arbitrage et par conséquent de diminuer les coûts[10].

Les sentences arbitrales sont exécutoires en vertu de la Convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères[11], signée par plus de 100 pays, qui permet d'imposer l'exécution des sentences arbitrales étrangères, mais prévoit quelques exceptions. L'application des sentences arbitrales étrangères d'un jugement rendu par un tribunal étranger est souvent moins compliquée et coûte moins cher que l'exécution dans un pays qui ne le reconnaîtra peut-être pas ou n'en permettra pas l'exécution.

Enfin, à quelques exceptions près[12], l'arbitrage ne relève pas du domaine public, contrairement à la plupart des poursuites en justice. La conduite de la procédure et les décisions ne sont habituellement pas rendues publiques, ce qui peut constituer un avantage important.

Inconvénients de l'arbitrage

L'arbitrage suppose un consensus. Si l'une des parties refuse de s'y soumettre, elle ne peut y être contrainte. De plus, l'arbitrage est une procédure longue et coûteuse, qui n'établit pas de précédent, de sorte qu'il se peut fort bien que les parties aient à demander plusieurs fois l'arbitrage du même litige, avec des parties différentes.

Des questions complexes surgissent souvent dans le règlement d'un litige qui implique les droits des tiers. Sans le consentement à l'arbitrage du tiers, l'arbitre n'a pas autorité pour prendre une décision qui lie celui-ci. Dans ce cas, la procédure de recours appropriée serait la poursuite en justice, dans l'hypothèse où les tribunaux auraient compétence à l'égard des tiers. Par conséquent, dans un contrat interentreprises où la véritable question concerne les droits d'un tiers (par exemple la personne concernée par les données), il se peut que l'arbitrage ne constitue pas une méthode utile de règlement du litige.

Médiation

La médiation repose sur une procédure structurée à laquelle contribue un tiers indépendant. L'autorité du médiateur est consensuelle. Le médiateur aide les parties en litige à prendre en compte leurs intérêts respectifs et à identifier des possibilités de règlement, mais il ne peut privilégier une issue par rapport à une autre ni imposer une décision. De nombreuses organisations aident les parties qui cherchent la médiation. En général, une partie peut se retirer de la médiation à tout moment.

Avantages de la médiation

La médiation est une méthode moins formelle pour résoudre les litiges. Les parties sont libres de choisir un médiateur qui fait autorité dans un domaine en particulier et de s'entendre sur la législation applicable ou les principes d'autorégulation ou codes de conduite qui régiront la médiation, ce qui leur laisse davantage de liberté que dans un recours en justice traditionnel. La souplesse de la procédure permet aux parties de trouver des solutions créatives et novatrices à leurs litiges.

Dans une médiation, les parties sont libres de verser un élément de preuve ou de présenter une information qui pourrait contribuer au règlement du litige. Elles peuvent souvent s'entendre plus rapidement et à moindre coût que devant une instance plus traditionnelle de règlement. La médiation implique généralement moins de contestation et pourrait être la méthode idéale pour régler un litige quand les parties souhaitent poursuivre leurs relations d'affaires.

Inconvénients de la médiation

La médiation, si elle réussit, aboutit à une transaction. Ce type d'accord pourra être rendu exécutoire par de nombreux tribunaux. Toutefois, dans d'autres juridictions il se peut que les tribunaux se déclarent incompétents pour les faire exécuter.

Par ailleurs, la médiation n'aboutit pas toujours à un accord. Les parties peuvent choisir cette voie, mais si elles ne parviennent pas à s'entendre, elles devront recourir à d'autres moyens, tels la procédure judiciaire ou l'arbitrage[13].

Les résultats d'une médiation peuvent aussi être très variables, même pour des litiges de nature très semblable.

La médiation-arbitrage

Dans une procédure de médiation-arbitrage, les parties s'entendent pour essayer d'abord de régler le litige par la médiation et, en cas d'échec, pour soumettre leur litige à un arbitre.

Cette solution a l'avantage de permettre aux parties de faire d'importantes économies de temps et d'argent si elles parviennent à s'entendre par la médiation, tout en préservant leur droit à l'arbitrage en cas d'échec. Généralement, la médiation-arbitrage offre de meilleures chances de succès lorsque les parties fixent un délai au processus de médiation, au terme duquel elles auront recours à l'arbitrage.

Mini-trial et expertise

Il existe deux autres formes de mécanismes alternatifs de règlement : le mini-trial (procès simplifié) et l'expertise. Dans le premier cas, les parties se rencontrent en présence d'un tiers qui, après avoir entendu le fond du litige, donne une opinion impartiale sur la manière probable dont le tribunal statuerait. Le but visé est de favoriser un règlement volontaire entre les parties. Dans le second cas -- l'expertise --, les parties s'en remettent à un expert auquel elles soumettent certaines questions clés. Les parties peuvent ensuite inclure les conclusions de l'expert dans un processus subséquent ou une convention qui les liera[14]. Ces deux méthodes ont l'avantage d'être rapides et rationnelles du point de vue des coûts. Elles sont utilisées de manière volontaire et le résultat auquel elles aboutissent n'engage pas les parties, à moins que celles-ci ne décident d'inclure les conclusions de l'expert dans un accord exécutoire.

Mécanismes d'exécution

Mécanismes d'exécution conventionnels

Même si l'action en justice est le recours ultime, la question de l'exécution du jugement demeure. Malgré des accords internationaux comme la Convention de Bruxelles et des dispositions nationales comme celles qui aux États-Unis prévoient qu'un État doit accorder « pleine foi et crédit » aux procédures judiciaires des autres États, le problème de l'exécution d'un jugement prononcé à l'étranger demeure.

L'exécution des sentences arbitrales étrangères est régie par la Convention de New York, laquelle définit rigoureusement les motifs de non-exécution d'une sentence. Par conséquent, une partie qui obtient une sentence arbitrale pourra probablement la faire exécuter, sous réserve que le pays d'exécution soit signataire de la Convention.

Mécanismes d'exécution en ligne

Divers mécanismes de règlement des litiges en ligne ont été élaborés ces dernières années ; quelques-uns sont décrits ci-après. La question de l'exécution des décisions est traitée dans le cadre de certains de ces projets selon un processus graduel. Par exemple, BBBonline offre un programme d'arbitrage-médiation, lorsqu'un litige ne peut être résolu directement avec l'entreprise signataire.

Exemples de mécanismes de règlement des litiges en ligne

TRUSTe

TRUSTe[15] est un projet réputé visant à aider les consommateurs à résoudre les problèmes de protection de la vie privée et autres questions qui les préoccupent. Les propriétaires de sites Web peuvent signer avec TRUSTe un contrat d'un an, qui les oblige à respecter certains principes de protection de la vie privée et leur offre des procédures d'intervention progressives pour les aider à régler leurs litiges. TRUSTe vérifie que les sites Web respectent ses principes en matière de vie privée. Un mécanisme de règlement des litiges permet à TRUSTe d'étudier les cas et d'accélérer le cas échéant le processus de règlement d'un litige.

BBBonline

Dans une optique analogue, BBBonline[16] a été fondé pour contribuer à renforcer la confiance des consommateurs dans le commerce électronique. Le programme de protection de la vie privée de BBBonline offre une procédure d'évaluation complète qui permet de mesurer la capacité d'une entreprise à tenir les engagements qu'elle a pris dans sa déclaration de politique de protection de la vie privée en ligne, et propose un processus de règlement des litiges lorsque le consommateur a des inquiétudes au sujet de ses données personnelles.

OMPI

Le Centre d'arbitrage et de médiation de l'Organisation mondiale de la propriété intellectuelle (OMPI) propose des services de règlement des litiges portant sur l'utilisation et l'enregistrement abusifs de noms de domaine sur Internet, couramment appelés *cybersquatting*. Ces services de règlement des litiges se fondent sur les Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine, adoptés par l'*Internet Corporation for Assigned Names and Numbers* (ICANN). La Procédure s'effectue en grande partie en ligne[17], et il est également possible de soumettre les plaintes directement en ligne. La procédure prend 45 jours en moyenne, pour un montant minimal de USD 1 500 .

CRDP

Le Centre de recherche en droit public (CRDP) de l'Université de Montréal a lancé un projet expérimental, le CyberTribunal[18], qui avait pour but d'aider les parties à prévenir et à régler les litiges se produisant dans le cyberespace, et visait à répondre aux besoins des entreprises comme à ceux des consommateurs. Ce projet a pris fin en décembre 1999, mais il se prolonge dans un autre projet, sur lequel on peut se renseigner à l'adresse suivante : www.eresolution.ca.

NCAIR

Le *National Centre for Automated Information Research* (Centre national de recherche sur l'information automatisée) (NCAIR) a lancé le Projet de tribunal virtuel ainsi que le Bureau de l'Ombudsman en ligne, afin d'aider les parties à résoudre leurs litiges en ligne.

Virtual Magistrate

Virtual Magistrate[19] est un projet de service d'arbitrage entre utilisateurs de systèmes en ligne qui se plaignent de préjudices causés par certains contenus publiés sur l'Internet et par les opérateurs de systèmes. Les deux parties doivent consentir à la procédure, et les plaintes traitées ne peuvent porter que sur des questions comme la violation du droit d'auteur, la diffamation et l'atteinte à la vie privée.

Bureau de l'Ombudsman en ligne

Le Bureau de l'Ombudsman en ligne[20] (OOO) offre sur son site Web de l'information concernant le règlement des litiges. Les utilisateurs peuvent également demander de l'aide au service d'Ombudsman en ligne. Si ce service ne donne pas d'avis juridique, il suggère en revanche des stratégies à adopter pour parvenir à régler le litige.

Nécessité d'adapter les mécanismes de règlement des litiges aux transferts en ligne consommateur-entreprise

Déterminer à l'avance le processus de règlement des litiges

Pour susciter la confiance des consommateurs, le fournisseur de services, hormis lorsqu'il agit en tant que consommateur, devrait préciser clairement quels sont les codes de conduite et mécanismes alternatifs de règlement des litiges auxquels il souscrit, et la façon dont il est possible de s'informer sur ces codes et mécanismes.

Privilégier une attitude pragmatique

Dans un contrat interentreprises, les parties ont la possibilité de s'entendre contractuellement pour déférer à un processus de règlement des litiges. En revanche, de par la nature même de la navigation sur le Web, il serait peu réaliste d'imaginer que le consommateur moyen va s'intéresser à la question du règlement d'un éventuel litige avant d'interagir sur le Web. Cependant, afin de favoriser la confiance des consommateurs, les entreprises pourraient fort bien souhaiter promouvoir les mécanismes de règlement des litiges et les respecter.

Examen des options

La discussion antérieure sur les avantages et les inconvénients des mécanismes de règlement des litiges permet d'avancer que l'action en justice et peut-être l'arbitrage formel[21] sont des solutions de dernier recours, dont l'efficacité et la souplesse seraient limitées en ce qui concerne les contrats entre consommateurs et entreprises. Cependant, l'arbitrage pourrait trouver une application directe dans le règlement des litiges en ligne consommateur-entreprise, s'il était modifié pour s'apparenter davantage au recours à un arbitre tiers et était basé sur un ensemble de règles simplifiées.

Les autres options qu'il est intéressant d'explorer plus avant sont la médiation au sens strict, la médiation-arbitrage, l'expertise et la conciliation. Cette dernière catégorie est un hybride d'autres mécanismes. Sa structure exacte et son fonctionnement varient en fonction du modèle et reflètent des types particuliers de litiges. Le conciliateur a les pouvoirs tout à la fois d'un médiateur et d'un arbitre.

C'est ce qui distingue la conciliation des autres processus comme la médiation, qui peut prendre ensuite la forme de l'arbitrage (médiation-arbitrage).

Suggestions pour l'élaboration de mécanismes alternatifs de règlement des litiges en ligne entre consommateurs et entreprises

Développer des mécanismes de règlement des litiges pour les transactions en ligne entre consommateurs et entreprises exige l'examen de certains facteurs et des caractéristiques inhérentes à ces transferts. Quelques suggestions sont présentées ci-après comme éléments de réflexion.

Utilisation de déclarations de politique de protection de la vie privée

Une première suggestion serait d'encourager les entreprises à informer le consommateur sur les procédures de traitement ou d'instruction des plaintes qu'elles recommandent et sur la manière d'y recourir.

Le respect du mécanisme de résolution des litiges ainsi décrit pourrait être un des éléments à évaluer et à vérifier dès lors qu'une entreprise s'est soumise à un processus de vérification ou a demandé une certification. La vérification devrait donner un résultat tangible. De plus, ce service ne devrait pas être trop onéreux ou lourd à gérer.

Obligation d'épuiser tous les recours prévus

Les parties pourraient avoir l'obligation d'épuiser les recours prévus par le processus prescrit avant d'intenter une poursuite en justice.

Il existe des précédents pouvant être utiles, par exemple les procédures de règlement des litiges de certaines instances propres aux domaines de l'assurance, des télécommunications, des services bancaires et des services de santé. C'est seulement après que ces procédures ont été utilisées sans succès que le litige peut être porté en justice. Certaines réglementations sur la protection des données (tels les textes relatifs à la protection de la vie privée en Nouvelle-Zélande) stipulent que toutes les plaintes doivent d'abord être soumises aux autorités responsables de la protection des données pour instruction et/ou conciliation avant qu'on puisse passer au palier suivant du processus de règlement des litiges.

Une autre possibilité serait d'encourager le renvoi de tous les litiges à un service de règlement des litiges, sans toutefois rendre cela obligatoire. Les tribunaux seraient saisis en cas de nécessité pour les personnes concernées par les données, ou pour les consommateurs, d'obtenir une mesure d'urgence sous la forme d'un jugement avant dire droit ou d'une injonction, par exemple pour empêcher la diffusion de données à caractère personnel ou pour mettre un terme à une telle diffusion.

Choix des principes généraux sous-jacents

L'une des questions clés à examiner est de savoir si les mécanismes alternatifs de règlement des litiges entre consommateurs et entreprises devraient être consensuels, comme le sont la plupart d'entre eux, ou devraient offrir une solution d'arbitrage (avec l'autorité d'imposer une décision). Les options actuellement disponibles sont les suivantes :

- ***Évaluation par un expert indépendant (expertise) :*** les parties peuvent nommer un tiers indépendant, ou encore choisir parmi les experts d'un groupe proposé.
- ***Conciliation :*** ce processus est une combinaison de techniques de médiation et de procédures judiciaires qui implique parfois le recours à un expert indépendant. Le conciliateur peut faire des recommandations et parfois parvenir à un règlement. Cependant, si ses recommandations ne sont pas suivies, l'affaire est alors automatiquement aiguillée vers une autre procédure.
- ***Processus par étapes ou à deux volets :*** le processus de règlement des litiges peut commencer par une médiation, et s'il est impossible de parvenir à un accord, se poursuivre par un arbitrage.
- ***Arbitrage en ligne***.

Autres questions à examiner

Il importe également de se pencher sur un grand nombre d'autres questions, notamment :

- Le processus d'enregistrement et de notification des litiges.
- La notification aux parties, y compris l'information à leur transmettre et les règles qui régissent les communications ; la définition des critères applicables au fait d'entendre le litige.
- La nomination d'un groupe d'experts.
- La nomination du tiers (arbitre, médiateur, conciliateur ou expert).
- Les protocoles d'identification des transferts d'information ainsi que de tout document ou élément de preuve pouvant contribuer au règlement du litige.
- Les protocoles permettant d'établir le dossier de la procédure.
- La confidentialité.
- La sécurité des communications et la détermination des transmissions qui doivent être cryptées.
- Les possibilités d'admettre ou de faire participer des tiers, tels que :
    (a) Une autorité de protection des données.
    (b) Un agent de vérification, inspecteur ou vérificateur.
- L'interface avec toute action d'autorégulation ou voie de recours prévue par le code ou la réglementation de l'industrie.
- La capacité ou l'utilité de publier les décisions exécutoires, les commentaires de cas anonymisés, les informations donnant une orientation ou un point de vue, les statistiques, les rapports, ainsi que les preuves versées à la procédure.
- Tout pouvoir de prévenir le secteur ou organisme de l'industrie visé si le litige touche une catégorie de personnes ou révèle une pratique répandue (en matière d'atteinte à la vie privée).
- Les limites possibles des sanctions (telles les limites à l'indemnisation ou aux pouvoirs décisionnels particuliers de l'arbitre).

- En l'absence d'accord, le conseil fourni aux personnes concernées par le traitement de leurs données relatif aux autres voies de recours disponibles et à leurs droits.
- Les règles relatives à l'exécution de tout accord, décision ou sentence finale.
- L'autoévaluation du service. Les statistiques du service devraient être périodiquement réévaluées pour ce qui a trait notamment aux types de litiges, à leur règlement et aux raisons pour lesquelles certaines procédures sont choisies de préférence à d'autres. Les résultats de ces évaluations devraient servir à améliorer la conception du système de règlement des litiges.
- Le volume de litiges que toute procédure pourrait traiter.
- La simplicité ou la complexité de la procédure, sa rapidité et son coût.
- Le besoin éventuel d'une procédure comportant plusieurs paliers, du traitement des plaintes à l'arbitrage.

D'autres questions telles que le financement, la gestion, la surveillance, la responsabilité et la qualité devraient également être examinées.

Conclusions sur les mécanismes de règlement des litiges

Les consommateurs comme les entreprises ont besoin d'avoir confiance dans les réseaux mondiaux qu'ils utilisent. Les uns et les autres ont besoin de mécanismes efficaces de règlement des litiges, y compris pour régler les questions de respect de la vie privée qui se posent lors des transferts de données en ligne entre entreprises et entre entreprises et consommateurs. Les questions de règlement des litiges sont cruciales pour le renforcement de la protection de la vie privée à l'échelle mondiale et il est important d'encourager l'élaboration de mécanismes adaptés au règlement des litiges en ligne entre entreprises et consommateurs.

Bien que certains des mécanismes traditionnels puissent être modifiés pour mieux s'adapter au règlement des litiges en ligne, il est probable qu'il faudra élaborer de nouveaux mécanismes. Pour les transactions entre entreprises et consommateurs et entre PME, le coût, la rapidité, l'efficacité et le caractère exécutoire des mécanismes de règlement des litiges sont des éléments importants à considérer.

VI. Initiatives futures

Sommaire des conclusions

Les conclusions du présent rapport montrent que les solutions contractuelles ont un rôle à jouer pour la protection de la vie privée dans le contexte des flux transfrontières de données sur les réseaux électroniques mondiaux. Il convient de noter à cet égard que les contrats interentreprises permettent de satisfaire aux exigences des divers instruments de protection de la vie privée. Ces contrats, comme le fait ressortir le rapport, ont leurs limites. Ces dernières ne sont toutefois pas assez importantes pour remettre en cause la valeur des solutions contractuelles comme outil de protection de la vie privée. Par un effet cumulatif, les contrats devraient contribuer à l'amélioration des pratiques en matière de traitement de l'information et garantir les flux transfrontières de données d'une manière d'autant plus importante que des mesures complémentaires de protection de la vie privée sont mises en œuvre.

De nombreuses questions relatives aux contrats interentreprises sont également pertinentes pour ce qui concerne les transferts entre consommateurs et entreprises. Néanmoins, les pressions et caractéristiques inhérentes à l'infrastructure mondiale de l'information ont des implications considérables sur l'utilisation de solutions contractuelles pour protéger la vie privée.

Le rapport a mis en évidence un certain nombre d'initiatives dont l'étude mérite d'être poursuivie. Quatre thèmes se dégagent des conclusions :

- L'importance de la promotion de la protection de la vie privée et la nécessité de proposer des outils éducatifs.
- Les moyens d'élaborer et de faire respecter des engagements en matière de protection de la vie privée dans le cadre des transferts consommateur-entreprise en ligne.
- Les divers développements intervenant au niveau international qui nécessitent un suivi et une collaboration ultérieure.
- La nécessité d'élaborer des mécanismes alternatifs de règlement des litiges concernant les transferts électroniques entre consommateurs et entreprises.

Promouvoir la protection de la vie privée et les outils pédagogiques

Conformément au Principe de transparence énoncé dans Lignes directrices de l'OCDE sur la protection de la vie privée, il importe de privilégier en permanence des mesures systémiques visant à améliorer les procédures, selon le cas, d'information et/ou d'obtention de consentement, pour assurer transparence et responsabilité. Les personnes concernées doivent être informées des finalités de la collecte et du traitement de leurs données. C'est une condition essentielle pour qu'elles puissent contester le cas échéant l'exactitude des données les concernant et l'utilisation qui en est faite, et faire valoir leurs droits, par exemple en exerçant un recours.

Le générateur de déclaration de politique de protection de la vie privée de l'OCDE constitue à cet égard pour les entreprises une mesure concrète qui, par les moyens qu'elle offre, contribue à les sensibiliser à leurs responsabilités en matière de protection de la vie privée. Le générateur de l'OCDE permet aussi à ces entreprises (aux maîtres des fichiers) de structurer leur politique de protection de la vie privée. Il convient d'encourager cette dimension pédagogique du générateur, en insistant sur la corrélation qui existe entre d'une part le respect des principes de l'OCDE concernant la protection de la vie privée par les personnes responsables du traitement des données personnelles, et d'autre part le renforcement de la confiance du consommateur face au cyberespace.

S'agissant de la sensibilisation des personnes concernées, il pourrait être envisagé d'exploiter les possibilités de la technologie pour créer un site Web spécialisé dans la diffusion qui offrirait aux personnes concernées toutes ressources utiles concernant la législation et les mécanismes d'autorégulation.

Engagements exécutoires à l'égard de la protection de la vie privée dans le cadre des transferts électroniques entre consommateurs et entreprises

La collecte de données a lieu dans une large mesure avant qu'il y ait formation d'un contrat. Tant qu'un consommateur n'a pas répondu aux divers messages l'incitant à sélectionner les produits ou services d'un site, ou qu'il n'a pas transmis de renseignements concernant le paiement, il est très

difficile d'établir que le consommateur explorant un site Web et le maître du fichier de ce site ont eu l'intention de se lier par voie contractuelle.

Dans ce contexte, les déclarations de politique permettent aux maîtres des fichiers (propriétaires des sites Web) d'informer le consommateur de leurs obligations en matière de protection de la vie privée et de l'existence d'un certain nombre d'autres mesures garantissant le respect de ces obligations. Il peut s'agir des processus de vérification et de certification du site Web, de la compétence juridictionnelle et du droit applicable d'un pays donné, et la façon dont seront traitées les plaintes, en particulier du processus de règlement des litiges.

L'élaboration de mesures de protection de la vie dans un cadre contractuel pourrait poser des difficultés en raison des questions liées au facteur temps qui caractérisent les transferts entre consommateurs et entreprises. Même si la déclaration de politique était tenue pour avoir une valeur contractuelle, le consommateur devrait avoir la possibilité d'exercer un recours en vertu de ce contrat. Un particulier (une personne concernée) qui intentera des poursuites judiciaires selon la procédure classique contre une entreprise en ligne pour atteinte à sa vie privée se heurtera à maintes difficultés. Il serait peut-être plus efficace de miser moins sur les solutions contractuelles et davantage sur les mesures de règlement des litiges, notamment en établissant à cette fin des dispositifs novateurs d'autorégulation.

Suivi et coopération

Assurer le suivi de nombreuses évolutions internationales permettrait d'en tirer des enseignements utiles au moment de mettre en application des solutions contractuelles et des mesures complémentaires pour protéger la vie privée. Parmi les aspects qui devraient être suivis de près, il convient de retenir :

- Les développements liés au commerce électronique relatifs aux obligations contractuelles liées à l'acceptation, à la non répudiation et à l'authentification.
- Les expériences concrètes de divers types de mesures de vérification et de certification, en vue d'en évaluer l'aspect pratique, l'efficacité et les avantages.
- Toute initiative à venir fondée sur les clauses modèles de la CCI.
- Toute tentative de rationalisation des règles en matière de conflits de lois visant à prendre en compte les caractéristiques transfrontières de l'Internet et la difficulté de définir une territorialité selon des critères géographiques ou matériels.
- La tendance des pays à adopter des lois pour reconnaître le droit des tiers à avoir la qualité de bénéficiaire à un contrat (afin d'éviter les problèmes liés en l'absence de connexité contractuelle).
- Toute initiative de coopération internationale dans le domaine de la reconnaissance juridique de déclarations, d'énoncés ou autres formes de politique sur la protection de la vie privée qui décriraient les processus de règlement des litiges à suivre.
- Les divers projets dans le monde portant sur l'élaboration de mécanismes de règlement des litiges en ligne.

Cadre possible pour l'élaboration de mécanismes appropriés de règlement des litiges en ligne entre consommateurs et entreprises

L'importance des recours des particuliers en cas d'atteinte à la vie privée semble un thème récurrent. Indépendamment du fait que l'on puisse ou non appliquer un cadre contractuel à la collecte de données sur le Web, on constate un besoin urgent d'assurer une meilleure protection de la vie privée aux particuliers dans les transferts consommateur-entreprise. Il importe par conséquent de faire en sorte que les consommateurs (ou les personnes concernées) puissent déposer une plainte qui fasse l'objet d'une enquête et à laquelle il soit donné suite sans pour autant qu'ils aient à suivre le processus long, complexe et coûteux d'un recours en justice. Les entreprises y trouveront également leur compte en termes de coûts et de temps, le processus de règlement des litiges sera plus facile à contrôler, et la crédibilité et le climat de confiance s'amélioreront. Tous ces facteurs militent en faveur de mécanismes alternatifs d'autorégulation qui permettraient de régler un grand nombre de litiges ayant trait aux transferts en ligne de consommateur à entreprise.

L'élaboration d'une déclaration de politique de protection de la vie privée pourrait permettre de définir en quoi consiste le traitement des plaintes et le processus de règlement des litiges. Il serait possible d'adapter un certain nombre de mécanismes, qu'il s'agisse de médiation (processus consensuel) ou de mesures arbitrales.

En conclusion, la nature même et l'envergure du support utilisé dans les transferts entre consommateurs et entreprises ne permettent pas de considérer que le contrat pourrait être une solution universelle. Il vaudrait mieux envisager une approche plus générale et élaborer des réponses adaptées à une stratégie globale de protection de la vie privée. L'OCDE pourrait utilement contribuer aux travaux futurs à cet égard en approfondissant certaines des questions mises en évidence dans le présent rapport, en particulier l'étude de mécanismes de règlement des litiges en ligne.

NOTES

1. Il s'agit des huit principes suivants : limitation en matière de collecte, qualité des données, spécification des finalités, limitation de l'utilisation, garanties de sécurité, transparence, participation individuelle, responsabilité.

2. *Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries*, 22 avril 1998.

3. www.ntia.doc.gov/reports/privacydraft/198dftprin.htm

4. Principe de la responsabilité. « Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus ». Lignes directrices de l'OCDE sur la protection de la vie privée, paragraphe 14.

5. Paragraphes 37-39 du rapport explicatif, clause 4 du contrat type.

6. C'est le cas des accords signés par Fiat (1989) et par la Deutsche Bahn (AG)/Citibank (1995)

7. Clause 4.

8. « *Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries* », 22 avril 1998.

9. Convention de Bruxelles de 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale. Convention de Rome (80/934/CEE) de 1980 sur la loi applicable aux obligations.

10. Par exemple, le Règlement d'arbitrage de la CCI prévoit que : « Les parties peuvent convenir de réduire les délais prévus par le présent Règlement ». Paragraphe 32.1 du Règlement d'arbitrage de la CCI entré en vigueur le 1er janvier 1998. Plusieurs autres instances arbitrales prévoient des modalités semblables en ce qui concerne les délais.

11. Convention pour la reconnaissance et l'exécution des sentences arbitrales étrangères (Convention de New York), 10 juin 1958, entrée en vigueur le 7 juin 1959.

12. Aux États-Unis, les sentences arbitrales peuvent être dans une certaine mesure revues par les tribunaux et font donc partie du domaine public.

13. Un grand nombre d'organisations nationales et internationales offrent des services de médiation, et diverses compétences juridictionnelles ont des lois en matière de médiation qui peuvent varier considérablement. Face à ces disparités, de nombreuses instances tentent d'élaborer des codes ou des textes de lois à titre de modèles. Aux États-Unis par exemple, l'*American Bar Association*, de concert avec la *National Conference of Commissioners on Uniform State Laws*, a élaboré une version préliminaire de loi uniforme sur la médiation (*Uniform Mediation Act)* visant à remplacer la combinaison actuelle des lois des États sur la médiation (www.abanet.org/dispute). En Australasie, des organismes comme le LEADR *(Lawyers Engaged in Alternative Dispute Resolution)* et des organisations professionnelles juridiques sont en faveur d'une uniformisation des codes d'éthique.

14. La Chambre de commerce internationale offre ce service par l'entremise de son centre d'expertise international (*ICC International Centre for Expertise*). Ce centre, créé en 1976, offre aux parties les services d'une grande variété d'experts pour les aider de diverses façons, y compris dans le règlement des litiges.

15. www.truste.org.

16. www.bbbonline.org

17. http://arbiter.wipo.int/domains/rules/.

18. www.cybertribunal.org

19. www.vmag.org.

20. www.ombuds.org/center/ombuds.html.

21. On présume ici que le modèle d'arbitrage en cause fait appel aux procédures générales et complexes de soumission à un tribunal arbitral compétent.

ANNEXE

OÙ TROUVER DES RENSEIGNEMENTS SUR LA PROTECTION DE LA VIE PRIVÉE

ADRESSES DES ORGANISATIONS INTERNATIONALES ET RÉGIONALES, AINSI QUE DES AUTORITÉS NATIONALES DE CONTRÔLE ET DES ORGANISATIONS S'INTÉRESSANT A LA PROTECTION DE LA VIE PRIVÉE[1]

ORGANISATIONS INTERNATIONALES ET EUROPÉENNES

CHAMBRE DE COMMERCE INTERNATIONAL
Secrétariat International
38, Cours Albert 1er
75008 Paris
France
Tél : +33 1 49 53 28 28
Fax : +33 1 49 53 29 42
Mél : icc@iccwbo.org
Site Web :www.iccwbo.org/home/news_archives/2001/dataflow.asp

COMMISSION EUROPÉENNE
Groupe consultatif juridique de la Commission européenne
Direction générale XV-E1 (Libre circulation de l'information et protection des données)
Rue de la loi 200 (C 107)
1049 Brussels
Belgique
Tél : +32 2 296 2264
Fax : +32 2 296 8010
Site Web : http://europa.eu.int/comm/internal_market/en/dataprot/

Directive 95/46/EC of the European Parliament and of the Council 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:
http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

CONSEIL DE L'EUROPE
Unité Protection des données
Département de droit public
Direction générale des affaires juridiques
Secrétariat général
67075 Strasbourg Cedex
France
Tél : 33 3 88 41 3174
Fax : 33 88 41 2764
Mél : data.protection@coe.int
Site Web : www.coe.int/dataprotection

Convention 108 - Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/1Treaties.asp#TopOfPage

1. Cette liste n'est pas exhaustive.

NATIONS UNIES
Haut Commissariat des Nations Unies pour les droits de l'homme
8-14 Avenue de la Paix
1211 Genève 10
Suisse
Tél : +41 22 917 3924
Fax : +41 22 917 0213
Site Web : www.unhchr.ch/hchr_un.htm

Principes directeur pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptés par l'Assemblée générale résolution de 45/95 du 14 décembre 1990: www.unhchr.ch/html/menu3/b/71_fr.htm

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES
Information, Computer and Communications Policy Committee
2 rue André-Pascal
75775 Paris Cedex 16
France
Tél : +33 1 45 24 82 00
Fax : +33 1 45 24 93 32
Site Web : www.oecd.org/sti/security-privacy

Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel : www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information
www.oecd.org/dataoecd/59/0/1946946.pdf

ORGANISATION MONDIALE DU COMMERCE
154 Rue de Lausanne
1211 Geneva 21
Switzerland
Mél : enquiries@wto.org
Site Web : www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm
www.wto.org/english/tratop_e/serv_e/_derived/sourcecontrol_gats_factfiction10_e.htm

AUTORITÉS DE LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

ALLEMAGNE[2]
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12
53131 Bonn (Bad Godesberg)
Tél : +49 228 - 819 950 or 01888 - 7799 - 0
Fax : +49 228 819 95 50
Mél : poststelle@bfd.bund400.de
Site Web : www.bfd.bund.de

German regional Privacy Commissioners
www.datenschutz.de/partner/

2. Virtual Privacy Office : Un service en commun des institutions de protection de la vie privée des pays suivants : Allemagne, Canada, Pays-Bas, Pologne, République slovaque et Suisse : www.datenschutz.de.

AUSTRALIE
Federal Privacy Commissioner
GPO Box 5218
Sydney NSW 2001
Tél : +61 2 9284 9800
Fax : +61 2 9284 96 66
Mél : privacy@privacy.gov.au
Web site: www.privacy.gov.au

AUTRICHE
Büro der Datenschutzkommission und des Datenschutzrates
Bundeskanzleramt
Ballhausplatz 1
1014 Vienna
Tél : +43 1 531 15 25 28
Fax : +43 1 531 15 26 90
Mél : georg.lechner@bka.gv.at
Site Web : www.ris.bka.gv.at/

BELGIQUE
Commission de la Protection de la vie privée
Boulevard de Waterloo 115 / Avenue de la Porte de Hal 5 - 8
Bruxelles 1060
Tél : +32 2 542 72 00
Fax : +32 2 542 72 12 / 7201
E-mail : privacy@euronet.be
Site Web : www.privacy.fgov.be

CANADA[2]
Federal Privacy Commissioner
112 Kent Street
Ottawa Ontario K1A 1HR
Tél : +1 613 995 24 10
Fax : +1 613 947 68 50
Mél : mai@magi.com
Site Web : www.privcom.gc.ca

Provincial / Territorial Privacy Laws, Oversight Offices and Government Organisations
www.privcom.gc.ca/information/comms_e.asp

CHINESE TAIPEI
Prosecutor, Bureau of Legal Affairs
The Ministry of Justice
130 Sec 1 Chung Ching
South Road
Taipei 100 ROC 100
Tél : +886 2 381 39 39
Fax : +886 2 311 49 00

DANEMARK
Registertilsynet
Christians Brygge 28 - 4
1559 Copenhagen V
Tél : +45 33 14 38 44
Fax : +45 33 13 38 43
Mél : sekretariatet@registertilsynet.dk
Site Web : www.registertilsynet.dk

ESPAGNE
Agencia de Protección de Datos
Paseo de la Castellana 41, 5a planta
Madrid 28046
Tél : +34 1 308 40 17
Fax : +34 1 308 46 92
Mél : rel.internacionales@agenciaprotecciondatos.org
Site Web : www.ag-protecciondatos.es

ESTONIE[3]
Estonia Inspection of Data Protection
Pikk 61
EE 10133 – Tallinn
Tel : +372 627 4135
Fax : +372 627 4137
E-mail : info@dp.gov.ee
Web site : www.dp.gov.ee

ÉTATS-UNIS
National Telecommunications & Information Adm.
US Department of Commerce - Room 4713
14th & Constitution Avenue NW
Washington DC 20230
Tél : +1 202 48 21 816
Fax : +1 202 50 18 013
Mél : privacy@ntia.doc.gov

Federal Trade Commission
6th & Pennsylvania Avenue, N.W.
Washington, DC 20580
Tél : +1 202 FTC-HELP (382-4357)
Fax : +1 202 326-2012 attn: CRC
Site Web : www.ftc.gov/index.html

Department of Commerce
International Trade Administration
Office of Information Technologies & Electronic Commerce
14th & Constitution Avenue, N.W.
Washington, DC 20230
Tél : +1 202 482-0216
Fax : +1 202 482-5522
Site Web : http://export.gov/infotech

Office of Management and Budget
Executive Office of the President
725 17th Street, NW
Washington, DC 20503
TeleTel : 1 202 395 3080
Fax : 1 202 395 3888
Web : www.whitehouse.gov/omb/

3. Liens aux institutions nationales responsables de la politique de données caractère personnel dans les pays suivants : Estonie, Hongrie, Lettonie, Lituanie, Pologne, République slovaque, République tchèque : Site Web : http://ceecprivacy.org (Site Web des autorités de protection de données à caractère personnel du l'Europe centrale et de l'Est).

ÉTATS-UNIS
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554
Tél : +1 202 418 0200
Fax : +1 202 418 0232
Site Web : www.fcc.gov/

Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220
Tél : +1 202 622 2000
Fax : +1 200 622 6415
Web : www.ustreas.gov/

United States Department of Health and Human Services
200 Independence Avenue, SW
Washington DC 20201
Tél : +1 202 619 0257
E-mail: hhsmail@os.dhhs.gov
Site Web : www.os.dhhs.gov/

FINLANDE
Office of the Data Protection Ombudsman
Albertinkatu 25 A, P.O. Box 315
00181 Helsinki
Tél : +358 9 259 8771
Fax : +358 9 259 87735
Mél : tietosuoja@om.fi
Site Web : www.tietosuoja.fi

Finnish Communications Regulatory Authority
Itämerenkatu 3 A, P.O. Box 800
00181 Helsinki
Tél : +358 9 69 661
Fax : +358 9 6966 410
Mél : info@ficora.fi
Site Web : www.ficora.fi

FRANCE
Commission Nationale de l'Informatique et des Libertés
21, rue Saint -Guillaume
75340 Paris Cedex 7
Tél : +33 1 53 73 22 22
Fax : +33 1 53 73 22 00
MiniTél : 36-15 code CNIL
Site Web : www.cnil.fr

GRÈCE
Data Protection Commission
Omirou 8
105 64 Athens
Tél : +30 1 33 52 601-5
Fax : +30 1 33 52 617
Mél : pdonos@dpa.gr
Site Web : www.dpa.gr

GUERNSEY
Peter R Harris C. Eng, MA, PhD, FBCS
Data Protection Commission
PO Box 642
Frances House
Sir William Place
St. Peter Port
GY1 1JE
Tél : +44 (0) 1481 742074
Fax : +44 (0) 1481 742077
Mél : dataprotection@gov.gg
Site Web : www.dataprotection.gov.gg

HAWAII
Director
Office of Information Practices
Department of the Attorney General
Leiopapa a Kamehameha
Room 304
235 South Beretania Street
Honolulu
96813-2437.
Tél : +1 808 586 1400
Fax : +1 808 586 1412
Site Web : www.state.hi.us/oip/rules_home_page.htm

HONG KONG
Privacy Commissioner
Office of the Privacy Commissioner for Personal Data (PCO)
Unit 2001, 20/F Office Tower, Convention Plaza
1 Harbour Road
Hong Kong – Wanchai
Tél : +852 2877 7168
Fax : +852 2877 7026
Mél : hkpcpd@pco.org.hk
Site Web : www.pco.org.hk

HONGRIE [3]
The Parliamentary Commissioner for Data Protection and Freedom of Information
1051 Budapest
Nádor u. 22.
Tél : +36 1 475 7186
Fax : +36 1 269 3541

ÎLE DE MAN
Isle of Man Data Protection Registrar
Office of the Data Protection Registrar
PO Box 69
Douglas
Ile de Man IM99 1EQ
Tél : +1624 661030
Fax : +1624 661088
Site Web : www.gov.im/odpr/

IRLANDE
Data Protection Commissioner
Block 4 Irish Life Centre
Talbot Street
Dublin 1
Tél : +353 1 874 85 44
Fax : +353 1 874 54 05
Mél : info@dataprivacy.ie
Site Web : www.irlgov.ie/justice/Publications/publications.htm

ISLANDE
Data Protection Commission
Ministry of Justice
Arnarvholl
150 Reykjavik
Tél : +354 560 90 10
Fax : +354 552 73 40
Mél : afgreidsla@dkm.stjr.is

ISRAËL
Registrar of Data Bases
Ministry of Justice
6 Hillel Street
P.O. Box 2808
Israel - Jerusalem 91027
Tél : +972 2 625 56 50
Fax : +972 2 622 27 80

ITALIE
Garante per la protezione dei dati personali
Largo del Teatro Valle, 6
00186 Roma
Tél : +39 06 - 68 18 61
Fax : +39 6 681 86 50
Site Web : www.privacy.it/normativ.html

JAPON
Ministry of Public Management, Home Affairs, Post and Telecommunications
2-1-2 Kasumigaseki
Chiyoda-ku Tokyo 100 – 8926
Tél : +81 3 5253 5359
Fax : +81 3 5253 5345
Mél : opinions-2002@soumu.go.jp
Web site: www.soumu.go.jp

JERSEY
Data Protection Registrar
Data Protection Registry
Morier House
Halkett Place
St Helier
JE1 1DD
Îles Anglo-Normanes
Tél : +1534 5023255
Fax : +1534 502399

LETTONIE [3]
Data State Inspection
Kr.Barona iela 5-4,
Riga, Latvia, LV 1050
Tél : +371 7223131
Fax : +371 7223556

LITUANIE [3]
State Data Protection Inspectorate
under the Ministry of Public Administration Reforms and Local Authorities
Gedimino Str. 27/2
2600, Vilnius
Tel: +370 5 212 75 32
Fax: +370 2 61 94 94
E–mail: jakstaite@is.lt
Site Web : www.is.lt/dsinsp

LUXEMBOURG
Commission à la Protection des Données Nominatives
Ministère de la Justice
Boulevard Royal , 15
Tél : +352 478 45 46
Fax : +352 22 76 61

NORVÈGE
Datatilsynet / The Data Inspectorate
P.O. Box 8177 Dep
0034 Oslo
Tél : +47 22 39 69 00
Fax : +47 22 42 23 50
Mél : postkasse@datatilsynet.no
Site Web : www.datatilsynet.no

NOUVELLE ZÉLANDE
The Office of the Privacy Commissioner
P.O. Box 466
Auckland
Tél : +64 9 302 21 60
Fax : +64 9 302 23 05
Mél : privacy@iprolink.co.nz
Site Web : www.privacy.org.nz

PAYS-BAS [2]
College Bescherming Persoonsgegevens (CBP)
Prins Clauslaan 20
P.O. Box 93374
2509 AJ The Hague
Tél : +31 70 381 13 00
Fax : +31 70 381 13 01
Mél : info@cbpweb.nl
Site Web : www.cbpweb.nl

POLOGNE [2, 3]
The Office of the General Inspector of Data Protection
PL. Powstancow Warsawy 1
00 030 Warsawa
Tel : +48 22 827 88 10
Fax : +48 22 827 88 11
E-mail : sekretariat@giodo.gov.pl or dif@giodo.gov.pl
Site Web : www.giodo.gov.pl

PORTUGAL
Commissao Nacional de Proteccao de Dados Pessoais Informatizados
Rua de Sao Bento 148
1200 Lisboa
Tél : +351 1 392 84 00
Fax : +351 1 397 68 32
Mél : cnpdpi@mail.telepac.pt
Site Web : www.cnpdpi.pt or www.cnpd.pt

RÉPUBLIQUE SLOVAQUE[2, 3]
Office for Personal Data Protection
Mr Pavol Husar - President
Odborárske nám. 3
817 60 Bratislava
Tél : +421 2 5023 9418
Fax : +421 2 5023 9441
Mél : statny.dozor@pdp.gov.sk or pavol.husar@pdp.gov.sk
Site Web : www.dataprotection.gov.sk

National Security Authority
Budatínska 30
850 07 Bratislava
Tél : +421 2 6869 9519
Fax : +421 2 6382 4005
Mél : info@nbusr.sk
Site Web : www.nbusr.sk

RÉPUBLIQUE TCHÈQUE[3]
Office for Personal Data Protection
Havelkova 22,
130 00 Praha 3
Tél : + 48 22 827 88 10
Fax : + 48 22 827 88 11
Mél : info@uoou.cz
Site Web : www.uoou.cz

ROYAUME-UNI
The Office of the Data Protection Registrar
Water Lane
Wycliffe House
Wilmslow
Cheshire SK9 5AF
Tél : +44 (0) 1625 - 53 57 11
Fax : +44 (0) 1625 524 510
Mél : data@wycliffe.demon.co.uk
Site Web : www.dataprotection.gov.uk

SLOVÉNIE
Ministry of Justice
Zupanciceva 3
1000 Lubjana
Tel : +386 61 17 85 549
Fax : +386 61 12 61 050
E-mail : Joze.Santavec@gov.si

SUÈDE
Datainspektionen
Fleminggatan, 14, 9th Floor
Box 8114
104 20 Stockholm
Tél : +46 8 - 657 61 00
Fax : +46 8 652 86 52
Mél : Datainspektionen@din.se
Site Web : www.din.se/index.html

SUISSE[2]
Préposé fédéral à la protection des données / Data Protection Commissioner
Feldeggweg 1
3003 Berne
Tél : +41 31 322 43 95
Fax : +41 31 325 99 96
Mél : info@edsb.ch
Site Web : www.edsb.ch

ORGANISATIONS NON GOUVERNEMENTALES

CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 Eye Street NW
Suite 1100
Washington DC 20006
Tél : +1 202 637 9800
Fax : +1 202 637 0968
Site Web : www.cdt.org/

ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street, Suite 725
San Francisco CA 94103-4832
Tél : +1 415 436 9333
Fax : +1 415 436 9993
Site Web : www.eff.org/

ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Ave SE
Suite 301
Washington, DC 20003
Tél : +1 202 544 9240
Fax : +1 202 547 5482
Mél : info@epic.org
Site Web : www.epic.org/

FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION
B.C. Freedom of Information and Privacy Association
#204-1929 West Broadway
Vancouver, B.C.
V6J 1Z3
Tél : +1 604 739-9788
Fax : +1 604 739-9148
Site Web : griffin.multimedia.edu/~fipa/

GLOBAL WEB SITE LIBERTY CAMPAIGN
Site Web : www.gilc.org/index.htm

INFORMATION TECHNOLOGY INDUSTRY COUNCIL
1250 Eye Street NW Suite 200
Washington, DC 20005
Tél : +1 202 737 8888
Fax : +1 202 638 4922
Site Web : www.itic.org

THE NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY
601 Pennsylvania Avenue NW, North Building 11th Floor
Washington, DC 20004-2601
Tél : +1 202 756 3385
Fax : +1 202 756 3333
Mél : jschall@practicalprivacy.org
Site Web : www.practicalprivacy.org/nbcpe/index.htm

ONLINE PRIVACY ALLIANCE
c/o Christine Varney
Hogan and Hartson
555 13th Street NW
Washington, DC 20004
Tél : +1 202 637 5600
Mél : webmaster@privacyalliance.org
Site Web : www.privacyalliance.org/

PRIVACY AND AMERICAN BUSINESS
2 University Plaza
Hackensack, NJ 07601
Tél : +1 201 996 1154
Fax : +1 201 996 1883
E-mail: pab@idt.net or ctrslr@aol.com
Site Web : www.pandab.org/

PRIVACY COUNCIL
1300 East Arapaho, Suite #300
Richardson, Texas 75081
Tel: +1 972 997 4001, or 866 P-Council (866.726.8624)
Fax : +1 972 997 4450
Mél : info@privacycouncil.com
Site Web : www.privacycouncil.com/

PRIVACYEXCHANGE.ORG
C/o Centre for Social and Legal Research
2 University Plaza, Suite 414
Hackensack, NJ 07601
Tél : +1 201 996 1154
Fax : +1 201 996 1883
Mél : ctrslr@aol.com or admin@privacyexchange.org
Site Web : www.privacyexchange.org/

PRIVACY FORUM
Vortex Technology
Woodland Hills
California
Tél : +1 818 225 2800
Fax : +1 818 225 7203
Site Web : www.vortex.com/privacy.html

PRIVACY INTERNATIONAL
Privacy International Washington Office
666 Pennsylvania Ave, SE, Suite 301
Washington, DC 20003
Tél : +1 202 544 9240
Fax : +1 202 547 5482
Site Web : www.privacy.org/pi

PRIVACY RIGHTS CLEARING HOUSE
3100 - 5th Ave., Suite B
San Diego CA 92101
Tél : +1 619 298 3396
Fax : +1 619 298 5681
Mél : prc@privacyrights.org
Site Web : www.privacyrights.org

WORLD WIDE WEB CONSORTIUM
Site Web : www.w3.org/

ORGANISATIONS DU SECTEUR PRIVÉ

AT&T
AT&T Corp.
The Platform for Privacy Preferences (P3P) Project
295 North Maple Avenue
Basking Ridge, NJ 07920
United States
Tél : +1 973 360 8607
Mél : lorrie@research.att.com
Site Web : www.research.att.com/projects/p3p/

BBBOnLine, Inc.
4200 Wilson Boulevard
8th Floor
Arlington, VA 22203
United States
Tél : (Reliability Seal Program) +1 703 247 9370
Tél : (Privacy Seal Program) +1 703 247 9336
Tél : (Online Privacy Dispute Resolution Intake Center) +1 888 679-3353
Fax : +1 703 276-8112
Site Web : www.bbbonline.org/about/contactinfo.html

DIRECT MARKETING ASSOCIATION
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700
Tél : +1 212 768 7277
Fax : +1 212 302 6714
Web site: www.the-dma.org/

JAPAN INFORMATION PROCESSING DEVELOPMENT CENTRE
Kikai Shinko Bldg, 3-5-8, Shibakoen, Minato-ku,
Tokyo, 105-0011
Japan
Tél : +81 3 3432 9387
Fax : +81 3 3432 9419
Site Web : www.jipdec.orjp/security/privacy

PRIVACY TIMES
P.O. Box 21501
Washington DC 20009
Tél : +1 301 229 7002
E-mail evan@privacytimes.com
Site Web : www.privacytimes.com/

TRUSTe
685 Market Street, Suite 560
San Francisco, CA 94105
United States
Tél : +1 415 618 3400
Fax : +1 415 618 3420.
Mél : inquiries@truste.org
Web site : www.truste.org

LES ÉDITIONS DE L'OCDE, 2, rue André-Pascal, 75775 PARIS CEDEX 16
IMPRIMÉ EN FRANCE
(93 2003 05 2 P) ISBN 92-64-10164-0 – n° 53250 2003