ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Annexes au rapport de l'OCDE sur les politiques pour Préarer le Futur de l'Economie Internet

OECD Ministerial Meeting
on the Future of the Internet Economy
Seoul, Korea, 17-18 June 2008

Hosted by KOREA COMMUNICATIONS COMMISSION


OECD

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements de 30 démocraties oeuvrent ensemble pour relever les défis économiques, sociaux et environnementaux, que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse et la Turquie. La Commission des Communautés européennes participe aux travaux de l'OCDE.

Table des matières

Annexe A.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES RELATIVES À LA CONVERGENCE ET AUX RÉSEAUX DE PROCHAINE GÉNÉRATION

Introduction

La numérisation du contenu, l'émergence de la propriété intellectuelle et l'adoption croissante du haut débit par les utilisateurs ont permis la convergence des réseaux, des services et des équipements à laquelle nous assistons aujourd'hui. Ces services convergés apparaissent souvent sur le marché sous la forme d'offres tri- ou quadri-services combinant données, télévision et téléphonie fixe et mobile. Avec l'évolution de l'Internet et la convergence des plateformes, il importe de plus en plus de s'assurer que les utilisateurs continuent de disposer d'un accès aisé à l'Internet observant le principe de "bout en bout"[1].

Les réseaux de prochaine génération (NGN) forment la plateforme facilitant la convergence. Le sigle "NGN" (en anglais) recouvre deux niveaux de réseau : *"le cœur de réseau"* et *"le réseau d'accès"*. Le cœur des réseaux de prochaine génération assurent les fonctions des couches d'application et de commutation pour une multitude de services, tandis que les réseaux d'accès de prochaine génération faciliteront la prestation de services innovants.

La convergence d'un éventail d'applications et de services auparavant distincts, comme la téléphonie, la vidéo et les communications de données sur un seul et même réseau entraîne d'importants changements dans la façon dont les réseaux sont construits et les services sont assurés. La dissociation en couches distinctes du cœur de réseau (fonctions d'acheminement, de contrôle, de service et d'application) permet la concurrence et l'innovation à chaque niveau horizontal de la structure du NGN, mais elle peut aussi créer pour les opérateurs de réseaux de fortes incitations commerciales à étendre l'intégration verticale et pourrait conduire à ce que ceux-ci tirent parti de leur pouvoir de marché pour évoluer entre ces couches. Dans le même temps, si les nouveaux réseaux de transport peuvent apporter aux utilisateurs des gains significatifs en termes de capacité et de symétrie de la bande passante, le développement des réseaux d'accès de nouvelle génération peut aussi créer de nouveaux obstacles à la concurrence et à l'investissement en fonction de la topologie des réseaux et du niveau d'investissement requis des opérateurs pour déployer ces nouveaux réseaux.

Les décideurs et régulateurs devront peut-être analyser et revoir l'efficacité des cadres politiques et réglementaires historiques en vue de tirer parti des retombées des réseaux d'accès de prochaine génération et de la convergence, tout en limitant le plus possible les coûts que pourraient éventuellement induire ces nouveaux

1. Où l'intelligence et la puissance de traitement d'un réseau résident aux extrémités, tandis que le réseau lui-même reste aussi simple que possible.

développements (voir le rapport de référence sur la *Convergence et les réseaux de prochaine génération*). Il ne faudrait pas que les cadres politiques historiques entravent la convergence, l'investissement ou le choix sur le marché. Les nouvelles technologies et les nouveaux services peuvent procurer des retombées significatives aux utilisateurs, mais les décideurs voudront certainement surveiller le déploiement de ces technologies, pour assurer le développement de la concurrence sur ces marchés.

Deux objectifs majeurs devraient être pris en compte par les décideurs dans le suivi des cadres réglementaires :

- Buts économiques : la réglementation vise à instaurer des marchés véritablement concurrentiels et à encourager la poursuite de l'innovation et de l'investissement.
- Objectifs sociaux : nombre d'objectifs sociaux des cadres réglementaires existants seront sans doute considérés comme conservant leur pertinence dans un nouvel environnement technologique et de services. On peut évoquer à cet égard les questions liées au service universel, à l'accès, à la qualité de service, aux appels d'urgence, au pluralisme des médias, à la diversité culturelle et à la protection des consommateurs et autres utilisateurs.

On trouvera dans le présent document un certain nombre de principes dont les responsables de l'élaboration des politiques et les régulateurs au plan national pourraient s'inspirer pour relever les défis que posent actuellement la convergence et l'évolution vers la nouvelle génération de réseaux d'accès et du cœur de réseau.

Principes

1) Évolutions du marché : encourager l'investissement, la concurrence et la croissance

Les décideurs politiques devraient s'efforcer de créer un environnement favorable pour l'investissement et l'innovation et d'assurer aux participants sur le marché un environnement juridique et réglementaire prévisible. Dans ce contexte, ils pourraient prendre en compte un ensemble d'obstacles possibles à la concurrence et l'investissement susceptibles d'apparaître suite au déploiement des NGN. Il existe un certain nombre d'instruments pouvant aider à aplanir efficacement ces obstacles. Les décideurs devraient notamment :

- Reconnaître que les politiques et mesures réglementaires destinées à promouvoir la concurrence dans l'environnement des réseaux de prochaine génération devraient s'appuyer sur une solide évaluation économique des conditions spécifiques du marché et des facteurs locaux.
- Reconnaître que les régulateurs doivent envisager une possible domination du marché résultant du groupage de services.

De plus, si une concurrence adéquate au niveau des installations ne peut s'instaurer, dans les cas où le dégroupage de la boucle locale a été imposé, les décideurs devraient :

- Prendre en considération les difficultés que pourrait soulever le remplacement des réseaux d'accès par des réseaux de prochaine génération, qui pourraient créer de nouveaux goulets d'étranglement pour la concurrence, et contraindre ainsi les décideurs à prendre des mesures adéquates pour éviter toute discrimination indue dans l'accès à ces réseaux. Cet aspect revêt une importance particulière dans les pays qui s'appuient sur le dégroupage pour promouvoir la concurrence, dans la mesure où il pourrait être plus difficile de dégrouper de façon significative les réseaux d'accès de prochaine génération.
- Reconnaître que dans certaines circonstances une concurrence fondée sur les services pourrait constituer un premier pas important pour encourager la concurrence sur le marché et les investissements par les nouveaux entrants.
- Voir s'il convient d'assurer que les fournisseurs de services et d'applications disposent d'un accès non discriminatoire aux ressources du réseau, lorsque les choix en matière d'accès sont limités.

2) Accès à l'infrastructure passive

- Reconnaître que puisqu'une grande partie des coûts du déploiement des réseaux de fibre réside dans les travaux de génie civil, des politiques appropriées devraient être mises en place pour assurer un accès équitable et non discriminatoire aux fourreaux, pylônes et droits de passage. Des politiques devraient faciliter l'accès aux fourreaux et pylônes des opérateurs de télécommunications historiques (opérateurs de téléphonie fixe et mobile et câblo-opérateurs) et des entreprises de service public. L'accès aux droits de passage et fourreaux devrait être disponible sur une base non discriminatoire et fondée sur les coûts.
- Reconnaître que sans une concurrence adéquate au niveau des installations, le déploiement de la fibre plus près des abonnés pourrait introduire de nouveaux goulets d'étranglement, par exemple au niveau des armoires de raccordement et des réseaux de câblage internes dans les bâtiments d'habitation. Suivant les facteurs locaux, il se pourrait que ces nouveaux goulets d'étranglement imposent une action réglementaire, comme le dégroupage des sous-boucles et le partage des équipements de terminaison des lignes optiques dans les logements et bâtiments.

3) Neutralité de la réglementation vis-à-vis de la technologie

Suite à la convergence des réseaux et des services, il est important de faire en sorte que le marché soit ouvert à différentes technologies qui puissent rivaliser dans des conditions d'égalité. Dans ce contexte :

- Les gouvernements devraient encourager, dans toute la mesure du possible, le développement de réglementations neutres vis-à-vis de la technologie, notamment dans les domaines de convergence.
- Dans les secteurs du câble et de la téléphonie mobile, les régulateurs devraient voir si l'abandon des licences spécifiques à différentes technologies au profit de cadres d'autorisation neutres vis-à-vis des services serait bénéfique en termes de gestion efficiente de ressources rares,

d'allocation du spectre et de réalisation des objectifs d'intérêt public en la matière.

4) Interconnexion

L'interconnexion joue aussi un rôle important dans un environnement de NGN car elle doit intervenir à tous les niveaux fonctionnels afin que tous les prestataires de services puissent accéder aux nouveaux réseaux et proposer leurs contenus, services et applications aux utilisateurs. Des marchés commerciaux de l'échange de trafic IP se sont développés de façon satisfaisante sans intervention réglementaire. Les décideurs devraient donc :

- Suivre l'évolution future des marchés des NGN pour encourager un échange transparent et non discriminatoire de trafic entre les réseaux, et voir si une intervention réglementaire reste nécessaire.
- Réexaminer le fonctionnement et l'évolution du système d'interconnexion existant et suivre l'évolution dans la transition vers les NGN par des consultations auprès des professionnels et des utilisateurs.

5) Numérotage, nommage et adressage

Les adresses IP, les numéros de téléphone et les autres formes d'adresse sont des ressources essentielles pour la communication et l'accès au marché. En particulier, la disponibilité d'un nouvel espace d'adressage est nécessaire à la croissance de l'Internet. Les gouvernements devraient :

- Encourager l'introduction de la nouvelle version du protocole Internet (IPv6), en particulier par son adoption rapide par les pouvoirs publics de même que par les utilisateurs importants d'adresses Ipv4 du secteur privé, compte tenu de l'épuisement prochain des adresses IPv4.
- Revoir les plans de numérotage pour disposer de plus de souplesse, faciliter les nouveaux services convergés et améliorer le nomadisme des personnes.
- Suivre l'utilisation d'ENUM comme mécanisme de routage et d'interconnexion entre réseaux.

6) Allocation du spectre

Les technologies sans fil, notamment celles utilisant des fréquences non soumises à autorisation, deviennent un élément important du paysage des télécommunications. La gestion efficace du spectre est désormais une question clé pour les pouvoirs publics, avec l'augmentation rapide de l'éventail des technologies ayant des besoins de fréquences. Les décideurs pourraient ainsi être amenés à :

- Encourager la transition rapide vers la télédiffusion numérique et mettre des parties du spectre ainsi libérées (dividende numérique) à la disposition de services de communication et de radiodiffusion sans fil nouveaux et innovants.
- Reformer l'allocation du spectre et avoir recours à des mécanismes de marché et autres dispositifs reflétant la valeur économique du spectre sur les marchés des fréquences, en tenant compte dans les cas où cela est possible

d'objectifs d'intérêt public comme l'interopérabilité, l'encouragement de la diversité culturelle et linguistique et le pluralisme des médias.

- Revoir les structures institutionnelles pour la planification et l'allocation du spectre de telle manière qu'elles soient mieux coordonnées avec les besoins du marché et les exigences d'une régulation efficiente.

7) Service universel

Le service universel est un concept évolutif qui peut changer au fil des ans pour tenir compte des progrès dans les technologies et les usages. Les décideurs devront peut-être revoir les définitions du service universel pour déterminer si des changements doivent y être apportés et dans l'affirmative quels types de services et d'accès seraient exigés. Ils doivent également décider si les mécanismes de financement devraient être changés. Dans ce contexte, les gouvernements devraient :

- Revoir les obligations de service universel et les mécanismes permettant de les assumer dans le contexte de la convergence.
- Veiller à ce que les contributions aux fonds pour le service universel respectent l'évolution vers la convergence des réseaux et des services, et revoir la façon dont le service universel est financé.

8) Fracture numérique

Le déploiement des NGN pourrait créer des dissymétries en matière d'accès dans les régions non desservies par des infrastructures à large bande et haut débit. Il pourrait en résulter de nouvelles préoccupations quant à la compétitivité et à la croissance économique de ces régions.

- Les gouvernements devraient encourager le développement de réseaux à large bande et haut débit à l'échelle de tout leur territoire pour éviter de créer au plan national des dissymétries en matière d'accès, qui peuvent être particulièrement marquées entre zones urbaines et zones rurales. Dans ce contexte, il importe que les réseaux alternatifs soient encouragés. Les partenariats public-privé pourraient offrir une solution dans certaines zones pour réduire les coûts d'investissement, dans la mesure où le coût du câblage en fibre jusqu'au domicile dans les zones rurales et isolées peut être élevé compte tenu des coûts et des technologies du moment.

9) Services d'urgence

Il existe un risque accru de confusion sur la question de savoir si les utilisateurs ont ou non accès aux services d'appel d'urgence avec la convergence des plates-formes et des équipements, le développement de la mobilité et l'évolution vers les communications sur IP. Des mesures devraient être prises pour :

- S'assurer que les utilisateurs de services vocaux innovants sont correctement informés en ce qui concerne l'accès aux services d'urgence et qu'une forme ou une autre d'accès aux services d'urgence est garantie aux utilisateurs de services de VoIP. Ces dispositions devraient également prendre en considération les difficultés techniques de l'offre de ce type de service et ne

pas être une charge ou un obstacle excessif pour le développement d'applications et de services innovants.

10) Qualité de service

La qualité de service demeure importante dans un environnement de prochaine génération convergé où l'information emprunte plusieurs réseaux. Dans ce contexte, les décideurs devraient s'attacher à :

- Faire en sorte que la convergence profite aux consommateurs et aux entreprises, en leur offrant des choix suffisants en ce qui concerne la connectivité, l'accès et l'utilisation des applications, des équipements terminaux et du contenu sur Internet, de même que des informations claires et exactes sur la qualité et les coûts des services leur permettant de faire des choix en connaissance de cause.

11) Convergence des télécommunications et de la radiodiffusion

La convergence permet de distribuer via le même réseau, différents types de contenu et de services, qui peuvent être consommés via diverses plateformes et différents équipements terminaux. L'évolution de la technologie ne modifie pas nécessairement un grand nombre d'objectifs sociaux et culturels fondamentaux, mais elle pourrait modifier la façon dont ces objectifs sont réalisés. L'évolution de la technologie pourrait aussi permettre une plus grande libéralisation du marché, tout en maintenant les objectifs de base de l'action gouvernementale. A cette fin, les gouvernements devraient :

- Reconsidérer les obligations propres aux différentes plateformes à la lumière de la convergence des télécommunications et de la radiodiffusion, et élaborer des politiques plurimédias pour un environnement multiplateformes de manière à assurer la cohérence de la réglementation.
- Faciliter la diffusion de contenu via différents équipements.

12) Questions transfrontières

Les gouvernements devront peut-être prendre en considération certaines questions transfrontières liées au fait que les services sont de plus en plus indépendants des lieux et des réseaux. Les enjeux sont de taille pour les responsables de l'action publique. Ceux-ci pourraient notamment être amenés à :

- Réviser les cadres de protection des consommateurs et les mesures réglementaires relatives au contenu, à la protection des droits de propriété intellectuelle, à la protection de la vie privée et des données de caractère personnel et aux interceptions légales.

Annexe B.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES VISANT À PROTÉGER ET AUTONOMISER LES CONSOMMATEURS DANS LES SERVICES DE COMMUNICATION[1]

Au cours de la dernière décennie, le secteur des communications a évolué avec le développement de la concurrence et la diffusion de tout un éventail de technologies et services d'un type nouveau. La concurrence a eu d'importantes retombées pour les consommateurs avec la baisse des prix, l'amélioration de la qualité des services, l'élargissement du choix entre les prestataires de services et de l'accès à des services nouveaux. Les progrès dans les technologies et les services ont transformé la communication par des moyens électroniques en une fonction essentielle dans les pays de l'OCDE. Cette fonction essentielle sera accrue avec la mise en place d'infrastructures et de services de communication de prochaine génération. Les gains significatifs retirés par les consommateurs avec le développement de nouveaux services et de nouvelles technologies ont cependant été accompagnés d'un certain coût, dans la mesure où les consommateurs ont été confrontés à des choix plus complexes, à des éventails d'offres dont les structures tarifaires étaient parfois peu claires et à des contrats qui dans certains cas privaient les consommateurs d'une certaine flexibilité.

L'importance donnée à l'instauration de la concurrence sur les marchés des communications s'est principalement concrétisée par des mesures du côté de l'offre. Cependant, depuis quelques années, une prise de conscience croissante s'est développée selon laquelle les consommateurs disposant de davantage d'information et d'autonomie peuvent, par leurs choix au niveau de la demande, inciter les entreprises à innover, à améliorer la qualité des produits et services et à rivaliser sur les prix. En effectuant des choix éclairés entre les fournisseurs, les consommateurs tirent non seulement parti de la concurrence, mais ils la stimulent et l'entretiennent.

Dans le même temps, avec le développement des services de communication, une importance accrue est donnée au réexamen de la politique à l'égard des consommateurs en ce qui concerne les services de communication, afin de compléter l'éventail des mesures en faveur des consommateurs et de donner à ceux-ci davantage de protection, plus de souplesse sur le marché et un meilleur accès à l'information.

C'est dans ce contexte que les pays de l'OCDE ont élaboré un ensemble d'orientations pour les politiques visant à protéger les intérêts des consommateurs

1 . Par "communications" on entend ici les services des opérateurs de services de télécommunications, et les services d'accès à Internet et de communication par Internet fournis par les sociétés de télévision par câble et les fournisseurs d'accès à Internet.

dans les services de communication. Ces orientations reconnaissent nécessaire d'assurer une protection transparente et efficace des consommateurs tout en maintenant un environnement offrant des incitations à l'investissement dans les nouveaux services de communication. A cet égard, les principes contenus dans les présentes orientations pour les politiques doivent être lus au regard de ceux contenus dans les *Lignes directrices de l'OCDE de 1999 régissant la protection du consommateurs dans le contexte du commerce électronique*, des *Lignes directrices de l'OCDE de 2003 régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses* et de la *Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation*.

Les orientations pour les politiques de l'OCDE visent à :

a) Encourager le développement de services offrant aux consommateurs un éventail de produits de haute qualité à des tarifs concurrentiels.

b) Informer les consommateurs des risques potentiels pour la sécurité et la vie privée dans l'utilisation des services de communication, ainsi que des mesures disponibles pour limiter ces risques.

c) Accroître la sensibilisation des consommateurs à l'existence et aux avantages des services et fournisseurs disponibles et aux droits des consommateurs.

d) Améliorer la transparence des contrats et faire en sorte qu'ils ne soient pas inéquitables pour les consommateurs.

e) Minimiser les coûts associés au changement de services.

f) Faciliter le règlement rapide, peu coûteux, aisé, efficace et équitable des litiges de consommation.

g) Faire en sorte que les services soient largement accessibles à tous, et en particulier aux consommateurs désavantagés et vulnérables.

Dans ce contexte :

La complexité des services de communication, la pléthore de nouveaux services et le développement des offres groupées de services dans le cadre de contrats de longue durée font qu'il est de plus en plus difficile de comprendre et comparer les services.

- Les consommateurs de services de communication devraient recevoir des fournisseurs de services une information claire et exacte sur les modalités, conditions et coûts associés à ces services ; l'information devrait être aisément accessible et suffisante pour leur permettre de décider en toute connaissance de cause.
- La mise en place de ressources d'information de nature à aider les consommateurs à faire des choix éclairés et à accroître la sensibilisation de ces derniers au regard de leurs droits et des mesures de protection des consommateurs en la matière serait utile. Dans la mise en place de telles ressources, les besoins particuliers que peuvent avoir les consommateurs désavantagés ou vulnérables devraient faire l'objet d'une attention particulière.

- Les organisations indépendantes tierces et organisations de consommateurs devraient être encouragées à fournir des informations comparatives sur les prix/services qui aideront les consommateurs à faire des choix éclairés.

La qualité technique des services de communication fournis aux consommateurs peut varier de façon sensible. On peut également craindre dans certains pays que des opérateurs réduisent la qualité des services offerts aux consommateurs à de faibles niveaux, à l'insu des intéressés.

- Dans un souci de transparence, les opérateurs sont encouragés à informer les consommateurs de la qualité de leurs services et notamment, quand cela est réalisable, sur la variabilité de la qualité de ces services, afin de permettre aux consommateurs de faire des choix éclairés et de faciliter les décisions de changement de prestataire.

La disponibilité de numéros d'appel d'urgence et d'assistance téléphonique est parfois limitée ; certains numéros d'urgence qui peuvent être disponibles via les services téléphoniques traditionnels, par exemple, ne sont pas accessibles dans certains pays par téléphonie IP.

- L'accès aux services d'urgence et aux lignes d'assistance téléphonique devrait être assuré quelle que soit la nature du service de communication utilisé. Cette devrait prendre en considération les difficultés techniques de la fourniture de ces services et les limitations des services de communications non conçus pour remplacer la téléphonie vocale de base. Cette disposition ne devrait pas constituer une charge ou un obstacle excessif pour le développement d'applications et de services innovants. Toute limitation dans les services d'urgence fournis devrait être indiquée de façon claire et bien visible.

La possibilité pour les consommateurs de changer de prestataire de service est souvent entravée par les délais et les coûts que cela entraîne. Une réduction des coûts serait bénéfique pour les consommateurs et inciterait davantage les opérateurs à pratiquer des tarifs compétitifs et à améliorer la qualité du service.

- Les délais et les coûts associés au désengagement d'un service pour un autre par les consommateurs devraient être réduits le plus possible. Ainsi, les délais de préavis pour la résiliation des contrats et les périodes de verrouillage des téléphones portables pourraient être réduits pour faciliter le changement d'opérateur.

La portabilité du numéro joue un rôle important dans l'encouragement de la concurrence en éliminant le coût et les inconvénients d'avoir à changer de numéro de téléphone quand on change de prestataire. Elle réduit également les obstacles à l'adoption d'offres compétitives.

- La portabilité du numéro devrait être assurée et réalisée rapidement quand les consommateurs changent de prestataire, conformément à la politique de numérotation du pays.

Une absence d'interopérabilité obligeant les consommateurs à acheter du nouveau matériel pour utiliser les services d'un autre prestataire peut entraver le passage à un autre prestataire.

- Les parties prenantes devraient explorer les moyens d'accroître l'interopérabilité, en conciliant ce besoin avec celui de stimuler l'innovation des entreprises.

Le groupage de services peut être profitable pour le consommateur et, de fait, un nombre croissant de consommateurs optent pour des offres multiservices. Mais cela peut également constituer un frein si le consommateur souhaite changer de prestataire pour un service donné (par exemple, téléphonie ou Internet) et que cela l'oblige à changer également de prestataire pour l'ensemble des autres services.

- L'offre de services dégroupés devrait être considérée, lorsque cela est nécessaire, pour protéger la concurrence, ou préserver le choix du consommateur, tout en reconnaissant que les différences de tarifs entre offres groupées et services individuels sont souvent efficientes et profitables pour le consommateur.
- L'accès aux services de communication d'urgence devrait être assuré lorsque les autres services de l'offre groupée sont suspendus pour non-paiement.

Les prestataires de services de communication peuvent avoir recours à des pratiques de vente frauduleuses ou trompeuses. Il est arrivé que des utilisateurs soient victimes de slamming (écrasement de ligne sans autorisation) ; les contrats peuvent présenter des conditions restrictives et des exonérations (limitations de téléchargement, restrictions concernant l'accès au contenu) qui par ailleurs ne sont pas clairement indiquées dans la documentation promotionnelle. De plus, les campagnes de publicité et de marketing agressives qui exagèrent ou déforment les revendications peuvent être particulièrement préjudiciables à certaines catégories d'utilisateurs comme les enfants et autres consommateurs désavantagés ou vulnérables qui peuvent ne pas avoir la capacité de comprendre pleinement l'information présentée.

Conformément aux Lignes directrices de l'OCDE de 1999 régissant la protection des consommateurs dans le contexte du commerce électronique et aux Lignes directrices de l'OCDE de 2003 régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses :

- Les entreprises devraient fournir aux consommateurs des descriptions claires en ce qui concerne le contenu et les coûts des contrats.
- Les entreprises devraient être sanctionnées pour toute pratique de nature frauduleuse ou trompeuse.

Dans un certain nombre de pays, les contrats conclus avec les consommateurs sont souvent renouvelés automatiquement sans leur accord explicite, et parfois des modifications sont apportées aux conditions contractuelles sans préavis suffisant et sans information des consommateurs sur leur droit de rétractation en de telles circonstances.

- Les prestataires de services de communication devraient être encouragés à limiter la durée initiale des contrats, au-delà de laquelle une durée de préavis raisonnable devrait être prévue pour la résiliation du contrat.

- Les implications pour les consommateurs d'un consentement explicite ou implicite par défaut lors de la prorogation du contrat devraient être examinées plus en détail par les parties prenantes.
- Les consommateurs devraient être informés avec un préavis suffisant de toute intention de modifier les conditions contractuelles et de leur droit de rétractation en de telles circonstances.

Malgré les progrès de la technologie, les erreurs de facturation demeurent une cause majeure de plaintes des consommateurs.

- Le recours à l'autorégulation et aux codes de pratique professionnels pour la facturation est encouragé.
- Un suivi et/ou une intervention réglementaires peuvent être requis, le cas échéant, pour faire appliquer les mesures de protection des consommateurs.

Les consommateurs peuvent hésiter à engager des poursuites lorsqu'ils ont de graves différents avec leur prestataire de service, soit en raison du temps et de l'argent que cela nécessiterait soit parce qu'ils sont intimidés par la procédure judiciaire.

- Comme le prévoit la Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation, les consommateurs devraient avoir accès à des mécanismes de règlement des litiges et de réparation justes, aisés, rapides, efficaces et peu coûteux, y compris, quand cela est possible, à des services alternatifs de règlement des litiges.
- La mise en place d'organismes indépendants de règlement des litiges traitant des questions de services de communication devrait être encouragée.
- Les organisations volontaires de défense des consommateurs dont les fonctions pourraient porter sur l'assistance des consommateurs dans le règlement des litiges, pourraient être encouragées.
- Le rôle des instances de régulation dans le règlement des litiges devrait être explicité. Les fonctions des autorités de régulations doivent faire l'objet d'une large publicité.

Les nouveaux services de communication se sont également traduits par des risques accrus pour les consommateurs en termes de vie privée et de sécurité dans l'utilisation des réseaux et services. Les consommateurs doivent être conscients de ces risques et des mesures qui peuvent être à leur disposition pour se protéger.

Les prestataires de services de communication et les pouvoirs publics devraient informer les consommateurs des risques potentiels pour leur sécurité et leur vie privée auxquels ils pourraient être exposés lorsqu'ils utilisent des réseaux et services de communication, ainsi que des mesures disponibles qu'ils peuvent utiliser pour limiter ces risques.

- Les prestataires de services de communication devraient mettre en place des politiques et mesures de sécurité des données afin de prévenir les transactions non autorisées et les compromissions de données.
- Des mesures et des fonctions intégrées de sécurité devraient être développées.

Annexe C.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES RELATIVES A L'IDENTIFICATION PAR RADIOFRÉQUENCE (RFID)

Préface

Les technologies d'identification par radiofréquence (RFID)[1] sont de plus en plus utilisées. De nombreuses applications de la RFID sont mises en œuvre dans divers secteurs et à des fins très différentes. La RFID est parvenue à un stade où une plus large application laisse entrevoir des avantages qui pourraient être importants. Il subsiste cependant des obstacles qui justifient la mise en place d'un cadre pour les politiques destiné à accroître les effets bénéfiques de cette technologie au profit des entreprises et des consommateurs tout en prenant dûment en compte les questions de sécurité et de protection de la vie privée. Du point de vue des politiques publiques, un tel cadre doit créer des conditions propices, être neutre à l'égard des technologies RFID en reconnaissant leur diversité, et mettre en place les dispositions de base destinées à protéger les citoyens contre les effets négatifs de ces technologies, dès maintenant et à l'avenir. Ces principes pour les politiques reposent sur des études analytiques sur la RFID réalisées par l'OCDE entre 2005 et 2007[2].

La RFID est une technologie sans fil qui permet, au moyen d'un lecteur radiofréquence, de collecter les données contenues sur des étiquettes (ou « marqueurs », ou « puces ») électroniques qui sont apposées sur des objets ou y sont intégrées, notamment aux fins d'identification. Les systèmes RFID reposent sur l'utilisation de logiciels, de réseaux et de bases de données qui permettent la circulation de l'information entre les étiquettes et l'infrastructure informatique de l'organisation concernée, où l'information est traitée et stockée. Les systèmes mis en œuvre sont spécifiques aux applications. Certains utilisent des étiquettes passives relativement bon marché, avec une courte portée de lecture, qui ne contiennent elles-mêmes que peu d'informations, la plupart des données se trouvant au niveau du réseau. D'autres systèmes utilisent des étiquettes hautes performances qui offrent une grande capacité de stockage de données, sans connexion réseau, et une longue portée de lecture. A l'heure actuelle, les étiquettes haute performance restent moins viables commercialement mais leur coût diminue et elles font partie de systèmes de plus grande envergure, utilisant souvent la technologie des capteurs.

1. La RFID fait partie du groupe des technologies d'identification automatique et de capture de données, au même titre que les codes barres, la biométrie, les pistes magnétiques, la reconnaissance optique de caractères, les cartes à puce, la reconnaissance vocale et autres technologies apparentées.

2. Voir « L'identification par radiofréquences (RFID) : sécurité de l'information et protection de la vie privée » (2008) [DSTI/ICCP/REG(2007)9/FINAL], « Déploiement de la RFID : Possibilités offertes par la technologie et obstacles au déploiement : Étude de l'Allemagne » (2007) [DSTI/ICCP/IE(2007)6/FINAL], « Identification par radiofréquence (RFID) : Facteurs incitatifs, enjeux et considérations » (2006) [DSTI/ICCP(2005)19/FINAL], « Proceedings of the OECD Foresight Forum on Radio Frequency Identification Applications and Public Policy Considerations » (2005) [DSTI/ICCP(2006)7 disponible en anglais uniquement].

Des applications RFID sont utilisées depuis de nombreuses années dans différents secteurs d'activité : transports (pour gérer l'accès aux transports publics), contrôle d'accès (aux immeubles, aux autoroutes), billetterie et gestion événementielle, et plus récemment, cartes d'identité et passeports. Elles sont aussi très répandues dans la chaîne d'approvisionnement manufacturière et la logistique de distribution des produits. Le déploiement de la RFID varie grandement selon les secteurs d'activité. Les systèmes RFID sont très présents dans les secteurs automobile et hospitalier. Ils gagnent du terrain dans le commerce de gros et de détail, où l'on constate une évolution en faveur de stratégies d'application globale de cette technologie sur l'ensemble de la chaîne de valeur du secteur d'activité. L'essentiel de l'étiquetage s'effectue encore au niveau des palettes et des caisses de produits, mais il y a une tendance à l'étiquetage unitaire, en commençant par les biens et composants de grande valeur, en fonction de la baisse du prix des étiquettes.

Les avantages de ces applications pour les entreprises sont dans une large mesure spécifiques à chaque secteur d'activité, mais on peut en général retenir les suivants : optimisation des processus ; amélioration de leur qualité et de la sécurité, y compris recyclage et applications de lutte contre la contrefaçon ; amélioration de la gestion des stocks. La plupart des projets de mise en œuvre sont au stade initial et beaucoup d'entreprises doivent repenser leurs processus ou leurs méthodes de travail pour mieux tirer parti des avantages de la RFID. Des avantages de la RFID pour l'ensemble de la société sont également attendus dans divers domaines tels que la sécurité alimentaire, le rappel de produits, l'identification des médicaments, la santé publique et les applications médicales, la meilleure gestion des garanties, l'amélioration de l'information sur les produits et de la gestion des stocks.

Les progrès de la technologie sont axés pour l'essentiel sur l'amélioration de l'information en temps réel liée aux processus des entreprises, sur l'augmentation des performances des entreprises ainsi que sur les progrès en matière de sécurité et de protection de la vie privée. La combinaison de la RFID avec d'autres technologies laisse entrevoir d'intéressantes perspectives à plus long terme. Les technologies de communication et les capteurs permettront de suivre à distance les conditions ambiantes (par exemple, température, pression) dans des secteurs tels que la santé et l'environnement. Bon nombre des problèmes techniques qui se posent sont imputables aux lois de la physique : interférence radioélectrique, gestion de la puissance, réfléchissement, atténuation du signal.

Les problèmes que la RFID pourrait poser pour la société tiennent pour beaucoup à une caractéristique essentielle de la technologie : l'invisibilité des communications électromagnétiques qui ne rend pas évidente pour la personne qui porte le produit ou l'objet étiqueté la collecte d'information effectuée par des équipements RFID. Le contenu des étiquettes dépend des contextes d'utilisation. Par exemple, dans le contexte de la chaîne d'approvisionnement/distribution, les étiquettes attachées aux produits contiennent généralement une information qui identifie le produit et les questions de protection de la vie privée apparaissent après le point de vente ; dans les justificatifs d'identité, les puces peuvent parfois contenir des informations personnelles. La portée de lecture combinée des étiquettes et des lecteurs détermine dans quelle mesure les étiquettes peuvent être suivies. Des questions spécifiques concernent le contrôle de la lecture de l'étiquette, la protection des données personnelles, la possibilité de rapprocher des informations de localisation avec d'autres informations pour établir des profils de personnes et

l'usage possible des informations. Les questions à plus long terme concernent l'éventuelle omniprésence des lecteurs et des puces.

Comme toute autre technologie de l'information, la RFID n'est pas à l'abri de risques de sécurité[3] qui ont une incidence sur l'intégrité des systèmes, leur disponibilité et leur confidentialité, par exemple le déni de service, le brouillage, le clonage, l'écoute/interception et l'accès non autorisé aux données (« l'écrémage » ou *skimming*). Les systèmes RFID qui collectent et traitent de l'information relative à des personnes identifiées ou identifiables peuvent présenter des risques d'atteinte à la vie privée (par exemple, accès non autorisé à l'information stockée sur un marqueur). L'utilisation de la RFID pour la vérification d'identité, par exemple, suscite des craintes encore plus grandes en ce qui concerne la vie privée et il importe à cet égard d'assurer toute la protection nécessaire. Ces risques, s'ils ne sont pas pris en compte en amont, vont probablement alourdir le coût des applications RFID et, de façon plus générale, freiner l'adoption de cette technologie et en retarder par conséquent les effets bénéfiques.

Les *Lignes directrices de l'OCDE sur la sécurité*[4] et les *Lignes directrices de l'OCDE sur la protection de la vie privée*[5] constituent un cadre complet pour la sécurité des systèmes et réseaux d'information et la protection de la vie privée et des données personnelles. Ce cadre s'applique à la RFID.

Les principes pour les politiques énumérés ci-après constituent des orientations politiques et pratiques destinées à augmenter les avantages que les entreprises et les consommateurs peuvent tirer de l'utilisation de la RFID tout en tenant compte, de façon proactive, des questions de sécurité et de protection de la vie privée. Les Principes 1 à 6 portent sur les politiques et pratiques à mettre en œuvre par les gouvernements et les entreprises pour encourager l'utilisation de la RFID, maximiser ses avantages économiques et élargir ses applications et celles des nouveaux réseaux de capteurs. L'action publique est ainsi orientée vers : les mesures en faveur de la R-D et des technologies et applications génériques ; le développement d'applications du secteur public et le rôle des administrations publiques en tant qu'utilisateurs modèles ; l'information, la sensibilisation et l'éducation, notamment en ce qui concerne la protection de la vie privée et la sécurité, et l'utilisation de la RFID dans les petites entreprises ; l'harmonisation des normes ; et les problèmes d'allocation du spectre de fréquences. Les Principes 7 à 12 contiennent des orientations pour soutenir la mise en œuvre des *Lignes directrices sur la sécurité et sur la vie privée* pour toutes les parties prenantes lorsqu'elles déploient des systèmes RFID. Les questions spécifiques sont traitées relativement aux systèmes RFID ou aux composants RFID de systèmes plus vastes et incluent notamment la nécessité : d'une stratégie globale en matière de sécurité et de gestion de la vie privée ; d'évaluations

3. Par exemple, la reproduction de cartes de paiement RFID de type *Speedpass* et de clés de contact d'automobile.

4 . *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* (2002).

5 . *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* (1980).

des risques de sécurité et de l'impact sur la vie privée ; de mesures techniques de sécurité et de protection de la vie privée ; d'information des personnes ; ainsi que d'une politique générale de transparence. Le Principe 13 préconise un dialogue continu entre toutes les parties prenantes. Enfin, le Principe 14 met en évidence la nécessité de suivre l'évolution de la situation concernant la RFID.

Principes

1. Mesures en faveur de la R-D et de nouvelles applications

Les aides et incitations publiques devraient être concentrées sur la R-D sur les technologies et applications génériques liées à la RFID.

Bon nombre des domaines technologiques sur lesquels repose la RFID sont en cours de développement et de larges retombées économiques sont à attendre d'un effort de recherche soutenu dans des domaines essentiels au développement de la RFID, y compris la mise au point de nouveaux matériaux et de nouvelles technologies de lecture pouvant être utilisées sur de plus grandes distances, sans problèmes d'interférence et en environnement hostile. Il serait également utile pour la société de poursuivre la recherche sur les questions relatives à l'utilisation de la RFID dans les domaines des soins de santé et de l'environnement, par exemple sur les problèmes d'interférence avec d'autres appareils médicaux, l'impact des champs électromagnétiques sur les individus, ou l'effet des marqueurs sur les pratiques de recyclage. Il convient également d'encourager la recherche-développement axée sur des mesures techniques rentables intégrant aux systèmes RFID des dispositifs de sécurité et de protection de la vie privée (voir le Principe 9).

2. Neutralité technologique

Les politiques gouvernementales destinées à encourager l'utilisation et à accroître les avantages de la RFID doivent être neutres à l'égard des différentes technologies.

Les technologies et applications RFID sont très diverses et évoluent rapidement. Les premières varient en termes de capacité (par exemple, gamme de fréquences, autonomie de batterie et capacité de mémoire, taille). Les secondes couvrent un large éventail d'opérations et de secteurs d'activité différents. En voulant cibler les mesures sur des technologies ou applications particulières, on risque de réduire les ressources qui pourraient être consacrées à d'autres possibilités prometteuses et de fausser les marchés des composants et des équipements. Les politiques destinées à favoriser l'utilisation de la RFID et à en accroître les avantages ne devraient pas privilégier une technologie ou application par rapport aux autres.

3. Les administrations publiques comme utilisateurs modèles

Les administrations devraient partager le plus largement possible l'expérience acquise et les bonnes pratiques développées dans la mise au point et l'utilisation d'applications RFID à des fins d'intérêt général.

Les administrations mettent au point des applications novatrices de la RFID à des fins très diverses : traçabilité des œuvres d'art, gestion des inventaires de bibliothèques et de musées, gestion aéroportuaire et applications dans le secteur de la défense. L'expérience qu'elles acquièrent et les bonnes pratiques qu'elles développent à cet égard peuvent être bénéfiques pour d'autres acteurs et il convient de les partager aussi largement que possible afin de maximiser les retombées des investissements publics et de faciliter la diffusion de cette technologie.

4. Sensibilisation et information

Les administrations devraient encourager les initiatives pour faciliter la sensibilisation aux avantages de la RFID et aux défis qu'elle peut poser, et encourager le partage d'information sur les projets pilotes et de démonstration de grande envergure.

Les administrations, en collaboration avec les associations professionnelles, la communauté technique et, de plus en plus, les consommateurs et les autres groupes de la société civile, ont acquis de l'expérience en matière de sensibilisation aux avantages et aux problèmes liés aux applications émergentes des technologies, ainsi qu'à leurs impacts économiques et sociaux. La diffusion d'une information claire et neutre sur les technologies RFID, leurs caractéristiques et les aspects connexes concernant la sécurité et la protection de la vie privée, peut aider les petites entreprises et le grand public à apprécier les avantages et à mesurer les risques de ces technologies et à faire des choix informés en ce qui concerne leur utilisation. Les administrations devraient promouvoir la diffusion de ce type d'information dans les meilleurs délais, en particulier lorsque les applications ont des implications transsectorielles et un large impact social.

5. Normes

Il importe d'encourager l'élaboration de normes mondiales relatives à la RFID et reposant sur un consensus. S'agissant de la convergence des normes, il convient de recourir dans la mesure du possible à des mécanismes de marché.

L'élaboration et l'application de normes concernant les aspects techniques et la gestion de la RFID, à l'intérieur d'un même secteur et entre secteurs différents, favorise l'interopérabilité et l'apparition de nouveaux entrants sur le marché, et permet de réaliser des économies d'échelle dans les applications, en particulier au niveau international. Toutes les parties prenantes devraient être associées à l'élaboration de normes mondiales ouvertes et à l'harmonisation des normes sur la RFID tant à l'intérieur des secteurs qu'entre eux. Les normes peuvent aussi jouer un rôle important pour faciliter l'intégration de la sécurité et de la protection des données personnelles, et diffuser les bonnes pratiques concernant les systèmes RFID.

6. Spectre

Les pouvoirs publics devraient encourager et faciliter les applications RFID lorsqu'ils considèrent l'obligation de détenir une licence pour l'accès au spectre et son allocation.

Les pouvoirs publics, les fabricants, les organismes de normalisation et les autres parties prenantes devraient coopérer au niveau international pour assurer l'interopérabilité, pour considérer le cas échéant l'harmonisation des bandes de fréquences, pour limiter les interférences préjudiciables à d'autres utilisateurs et appareils radioélectriques et assurer que les systèmes fonctionnant sur les bandes de fréquences spécifiées soient conformes aux normes de puissance électrique et radio et à la politique fixée pour ces systèmes, et encourager le développement d'applications compatibles internationalement. L'exemption de licence pour l'utilisation des fréquences dans les applications RFID est une option reconnue comme favorisant l'adoption de la technologie RFID.

7. Gestion de la sécurité et de la protection de la vie privée

Les parties prenantes devraient adopter une optique globale pour élaborer une stratégie de gestion de la sécurité et, le cas échéant, de la protection de la vie privée, qui devrait être adaptée à chaque système RFID et prendre en compte les intérêts de toutes les parties concernées, y compris les particuliers.

Tous les systèmes RFID nécessitent l'élaboration d'une stratégie de gestion de la sécurité qui prenne en compte chaque étape de la vie du système (planification, mise en œuvre, exploitation, traitement des données et fin de vie) et chacun de ses composants (étiquettes et lecteurs, intergiciels, bases de données, réseaux et composants d'arrière-plan).

En revanche, tous ne nécessitent pas une stratégie de gestion de la protection de la vie privée, mais seulement ceux qui collectent ou traitent des informations relatives à une personne physique identifiée ou identifiable. Une organisation qui met en œuvre un système RFID devrait procéder à une analyse minutieuse pour déterminer si l'information RFID est constituée de données à caractère personnel (*par exemple*, nom ou identifiant personnel), ou si cette information RFID, bien que ne revêtant pas de caractère personnel (*par exemple*, identifiant d'objet), peut être mise en rapport avec une personne identifiée ou identifiable (*par exemple,* au point de vente). Dans un cas comme dans l'autre, le système RFID doit faire l'objet d'une stratégie de gestion de la protection de la vie privée couvrant chacune des étapes du cycle de vie des données RFID, du système et de chacun de ses composants.

8. Évaluations du risque de sécurité et de l'impact sur la vie privée

Les parties prenantes devraient procéder à une évaluation du risque de sécurité et, le cas échéant, de l'impact sur la vie privée et renouveler cette évaluation périodiquement.

L'évaluation du risque de sécurité et, le cas échéant, de l'impact sur la vie privée sont des outils essentiels pour gérer de la sécurité et la protection de la vie privée des systèmes RFID. Ces évaluations sont nécessaires pour déterminer les mesures, garanties et mécanismes de prévention et de réduction des risques, pour gérer le risque d'atteinte aux systèmes RFID, à l'organisation et aux personnes physiques, en tenant compte de la nature et de la sensibilité de l'information à protéger. Les évaluations de risque de sécurité et d'impact sur la vie privée devraient prendre en considération la technologie, l'application et les scénarios opérationnels. Elles devraient porter sur l'ensemble du cycle de vie des marqueurs RFID, y compris ceux qui demeurent fonctionnels bien que n'étant plus sous le contrôle de l'organisation.

L'évaluation de l'impact sur la vie privée d'un système RFID devrait déterminer s'il est nécessaire de collecter et de traiter de l'information relative à une personne identifiée ou identifiable. Elle devrait également prendre en compte la possibilité de lier à d'autres données les données collectées ou transmises au moyen de la RFID, ainsi que l'impact d'un tel rapprochement sur la personne concernée. Tout comme la question de la protection des données, cela revêt encore plus d'importance dans le cas de données personnelles sensibles (par exemple, données biométriques ou médicales, données d'identité). Enfin, les organisations pourraient envisager le cas échéant de rendre publiques leurs évaluations de l'impact sur la vie privée.

9. Mesures techniques de sécurité et de protection de la vie privée

Les parties prenantes qui élaborent ou exploitent des technologies et des systèmes RFID devraient intégrer des mesures techniques de sécurité et de protection de la vie privée à la conception et au fonctionnement de leurs systèmes.

Une combinaison de mesures techniques et non techniques est nécessaire pour assurer la sécurité et la protection de la vie privée dans le cadre de l'utilisation des technologies et des systèmes RFID. Des mesures techniques rentables intégrant des dispositifs de sécurité et de protection de la vie privée peuvent jouer un rôle important dans la réduction des risques et pour favoriser la confiance relative à ces technologies et systèmes. Un certain nombre de mesures sont déjà disponibles ou en cours d'élaboration (par exemple, désactivation, mécanismes d'authentification, cryptographie, minimisation et anonymisation des données). De plus amples efforts visant à faciliter leur adoption devraient être encouragés.

10. Information et consentement

Les parties prenantes qui utilisent la technologie RFID pour collecter ou traiter de l'information relatives à des personnes identifiées ou identifiables devraient le faire avec l'information des personnes concernées et, le cas échéant, avec le consentement de celles-ci.

Les personnes concernées devraient être informées de la collecte, du traitement, du stockage et de la diffusion de données RFID se rapportant à elles ou, le cas échéant, avoir la possibilité d'y consentir. Leur connaissance de ces opérations ou leur consentement devraient être fondés sur une compréhension de l'ensemble du cycle de vie des données RFID et pas uniquement de leur transmission initiale. Les

pouvoirs publics devraient encourager toutes les parties prenantes à s'efforcer de parvenir à un consensus sur les circonstances dans lesquelles le consentement de la personne concernée doit être ou non requis.

11. Notices d'information sur la protection de la vie privée

Les parties prenantes qui utilisent la technologie RFID pour collecter ou traiter des informations relatives à des personnes identifiées ou identifiables pourraient fournir dans les notices sur la protection de la vie privée davantage de renseignements que dans les notices habituelles de ce type, étant donné l'invisibilité de la collecte des données.

Outre l'information sur les données qui sont collectées, la finalité en vue de laquelle elles le sont et le droit d'accès à ces données, les notices sur la protection de la vie privée pourraient inclure la totalité ou certains des éléments d'information suivants : *i)* l'existence de marqueurs/étiquettes, *ii)* leur contenu, leur usage et leur contrôle, *iii)* la présence de lecteurs actifs, *iv)* la capacité de neutraliser les marqueurs et *v)* les coordonnées d'un service d'assistance. Ce type d'explication contribuerait également à sensibiliser le public à la nouvelle technologie. Il conviendrait d'encourager les activités de recherche axées sur des pratiques novatrices de notification, des notices normalisées et des moyens techniques pour améliorer la notification aux usagers.

12. Transparence

Les parties prenantes qui fournissent à des individus des étiquettes fonctionnelles — qu'ils collectent des données à caractère personnel ou non — devraient informer ces individus de l'existence de ces étiquettes, des risques d'atteinte à la vie privée qui y sont associés et de toute mesure prise pour limiter ces risques.

Les parties prenantes qui fournissent à des individus des étiquettes RFID qui demeurent fonctionnelles et qui pourraient être lues ultérieurement, y compris par des tiers, devraient appliquer une politique générale de transparence quant à l'existence de ces étiquettes, leur contenu et tout risque d'atteinte à la vie privée qu'elles pourraient poser en présence de lecteurs actifs, toute mesure pour prévenir ou réduire ces risques, notamment de l'information sur la façon de désactiver les étiquettes, les coordonnées de services d'assistance et tout autre renseignement pertinent. De plus, les personnes concernées doivent avoir la possibilité de neutraliser les étiquettes RFID en toute transparence, facilement et sans coût supplémentaire. Cependant, il est reconnu qu'il y a des circonstances spécifiques dans lesquelles la fourniture de telles informations pourrait se révéler impossible ou impliquer des efforts disproportionnés ou encore dans lesquelles il ne serait pas dans le meilleur intérêt des personnes concernées de neutraliser les équipements RFID.

13. Poursuite du dialogue

Les pouvoirs publics devraient encourager toutes les parties prenantes à poursuivre leurs travaux pour améliorer les politiques visant à renforcer les avantages économiques et sociaux que l'on peut escompter d'applications plus larges de la RFID et pour trouver des solutions efficaces aux problèmes qui subsistent en matière de sécurité et de protection de la vie privée.

Un dialogue suivi entre toutes les parties prenantes maximisera les avantages économiques et sociaux d'applications plus larges de la RFID et facilitera une meilleure sécurité et une protection de la vie privée accrue dans l'utilisation des systèmes RFID. L'utilité d'un tel dialogue a déjà été mentionnée, notamment en ce qui concerne la sensibilisation et l'information, la normalisation, la gestion du spectre des fréquences, le consentement des personnes et la transparence. L'élargissement du dialogue à l'élaboration, la diffusion et l'adoption de bonnes pratiques, notamment en matière de sécurité et de protection de la vie privée, faciliterait une diffusion plus large des technologies RFID et contribuerait à apaiser les préoccupations soulevées par leur éventuelle généralisation.

14. Regarder vers l'avenir : surveiller les évolutions

Les pouvoirs publics devraient encourager les travaux de recherche et d'analyse sur les impacts économiques et sociaux de l'utilisation de la RFID lorsqu'elle est associée à d'autres technologies et systèmes.

En raison du caractère continu de l'innovation technique, et de ses effets sur l'économie et la société, il est essentiel de suivre les évolutions et de déceler les tendances de la RFID dès que possible afin d'identifier les opportunités à saisir et les nouveaux défis à relever, et d'ajuster les politiques en conséquence. Les évolutions possibles de la RFID qui méritent d'être suivies à cet égard sont notamment la combinaison de cette technologie avec des systèmes reposant sur des capteurs, leur utilisation transnationale, la convergence de ces technologies sur l'Internet et leur éventuelle omniprésence.

Annexe D.
PRINCIPES ET LIGNES DIRECTRICES POUR L'ACCÈS AUX DONNÉES DE LA RECHERCHE FINANCÉE SUR FONDS PUBLICS

I. Objectifs

Ces *Principes et Lignes directrices pour l'accès aux données de la recherche financée sur fonds publics* (ci-après dénommés « *Principes et Lignes directrices* ») fournissent aux organismes publics d'élaboration de la politique scientifique et de financement des pays membres des recommandations générales sur l'accès aux données de la recherche financée sur fonds publics. Ils ont pour but de promouvoir l'accès aux données et leur mise en commun entre les chercheurs, établissements de recherche et organismes de recherche nationaux, tout en reconnaissant et en prenant en compte la diversité des lois, des politiques de recherche et structures administratives des pays membres.

L'objectif ultime des *Principes et Lignes directrices* est d'améliorer l'efficience et l'efficacité du système scientifique mondial, et non d'entraver son développement par de pesantes obligations et réglementations, ou d'imposer de nouveaux coûts aux systèmes scientifiques nationaux.

II. Champ d'application et définitions

Ces *Principes et Lignes directrices* visent les données de la recherche, déjà existantes ou à venir, qui sont subventionnées par des fonds publics pour produire des recherches et des connaissances scientifiques publiquement accessibles. Les *Principes et Lignes directrices* ne sont donc pas destinés à s'appliquer aux données de la recherche recueillies en vue de commercialiser les résultats de la recherche, ni aux données de la recherche qui appartiennent à une entité du secteur privé. L'accès à ces données fait intervenir tout un ensemble de considérations qui sortent du cadre du présent document. De plus, dans certains cas, l'accès aux données ou leur usage peut être limité afin de protéger la vie privée, la confidentialité ou des résultats couverts par un droit de propriété ou par la sécurité nationale.

Données de la recherche

Dans le cadre de ces *Principes et Lignes directrices*, les « données de la recherche » sont définies comme des enregistrements factuels (chiffres, textes, images et sons), qui sont utilisés comme sources principales pour la recherche scientifique et sont généralement reconnus par la communauté scientifique comme nécessaires pour valider des résultats de recherche. Un ensemble de données de recherche constitue une représentation systématique et partielle du sujet faisant l'objet de la recherche.

Ce terme ne s'applique pas aux éléments suivants : carnets de laboratoire, analyses préliminaires et projets de documents scientifiques, programmes de travaux futurs, examens par les pairs, communications personnelles avec des collègues et objets matériels (par exemple, les échantillons de laboratoire, les

souches bactériennes et les animaux de laboratoire tels que les souris). L'accès à tous ces produits ou résultats de la recherche est régi par d'autres considérations que celles abordées ici.

Ces Principes et Lignes directrices portent essentiellement sur les données de la recherche sur support numérique exploitable sur ordinateur. C'est en effet ce format qui offre le plus de possibilités d'améliorer la distribution efficiente des données et leur application pour la recherche, dans la mesure où les coûts marginaux de la transmission de données via l'internet sont pratiquement nuls. Les *Principes et Lignes directrices* pourraient également s'appliquer à des données de recherche sous forme analogique lorsque les coûts marginaux d'accès à ces données peuvent être maintenus à un niveau raisonnablement bas.

Données de la recherche financée sur fonds publics

Les données de la recherche financée sur fonds publics sont définies comme les données provenant de recherches menées par des organismes ou services publics ou à l'aide de fonds publics, quel que soit le niveau de gouvernement qui les fournit. La nature des « fonds publics » attribués pour la recherche étant très variable d'un pays à l'autre, ces *Principes et Lignes directrices* reconnaissent que ces différences plaident en faveur d'une approche souple de l'amélioration de l'accès aux données de la recherche.

Dispositifs d'accès

Les dispositifs d'accès sont définis comme étant le cadre réglementaire, stratégique et procédural mis en place par les établissements de recherche, les organismes de financement de la recherche et les autres acteurs concernés pour déterminer les conditions d'accès aux données de la recherche et d'utilisation de ces données.

III. Principes

A. Ouverture

Par ouverture, on entend l'accès dans des conditions d'égalité de la communauté scientifique internationale, à un coût le plus bas possible, de préférence ne dépassant pas le coût marginal de la diffusion. L'accès ouvert aux données de la recherche financée sur fonds publics devrait être aisé, rapide, convivial et passer de préférence par l'internet.

B. Flexibilité

La flexibilité suppose de prendre en compte les évolutions rapides et souvent imprévisibles des technologies de l'information, les caractéristiques de chaque domaine de recherche et la diversité des systèmes de recherche, des systèmes juridiques et des cultures de chaque pays membre. Les implications nationales, sociales, économiques et réglementaires spécifiques devraient être analysées lorsque des organisations conçoivent des dispositifs d'accès aux données de la recherche, et lorsque les gouvernements élaborent des politiques pour promouvoir l'accès aux données et examinent la mise en œuvre de ces *Principes et Lignes directrices*.

C. Transparence

L'information sur les données de la recherche et les organisations productrices de données, la documentation sur les données ainsi que les spécifications des conditions qui régissent leur utilisation devraient être accessibles au plan international, en toute transparence, dans l'idéal via l'internet. Le manque de visibilité des sources de données de recherche existantes et futures fait sérieusement obstacle à l'accès.

Les facteurs à considérer pour assurer la transparence sont notamment les suivants :

- L'information sur les organisations productrices de données ainsi que sur les données qu'elles détiennent, leur documentation concernant les ensembles de données disponibles et les conditions d'utilisation de ces données devraient pouvoir être aisément accessibles sur l'internet.
- Les organisations de recherche et les institutions publiques de recherche devraient activement diffuser l'information relative à leurs politiques en matière de données de la recherche auprès des chercheurs, des associations académiques, des universités et des autres acteurs de la recherche financée sur fonds publics.
- Chaque fois que cela peut être utile, tous les membres des divers milieux de la recherche devraient contribuer à établir des accords sur des normes de catalogage des données. L'application des normes existantes devrait être envisagée, dans la mesure du possible, pour éviter de solliciter davantage les ressources de la recherche et d'accroître la charge de travail des chercheurs et de leurs institutions.
- Des informations devraient être échangées sur la gestion des données et les conditions de leur accès entre les institutions chargées des archives de données et celles productrices de données, de manière à mettre en commun les pratiques exemplaires.

D. Conformité au droit

Les dispositifs d'accès aux données devraient respecter les droits et intérêts légitimes de tous les acteurs de l'activité de recherche publique.

L'accès à certaines données de la recherche et leur utilisation seront nécessairement limités par divers types de prescriptions légales, qui peuvent imposer des restrictions pour raisons de :

- Sécurité nationale : certaines données relatives au renseignement, aux activités militaires ou à la prise de décision politique peuvent être classifiées et partant, soumises à un accès limité.
- Protection de la vie privée et confidentialité : les données relatives aux sujets humains et d'autres données personnelles font l'objet d'un accès limité en vertu des législations et des politiques nationales de protection de la confidentialité et de la vie privée. Il convient toutefois que les détenteurs de ces données envisagent des procédures d'anonymisation ou de confidentialité permettant d'assurer un niveau de confidentialité satisfaisant afin de préserver autant que possible l'utilité des données pour les chercheurs.

- Secrets commerciaux et droits de propriété intellectuelle : les données concernant les entreprises ou autres parties, ou provenant de celles-ci, qui contiennent des informations confidentielles peuvent être inaccessibles pour la recherche.
- Protection d'espèces rares, menacées ou en danger : dans certains cas, il peut exister des raisons légitimes de limiter l'accès aux données sur la localisation de ressources biologiques en vue d'assurer leur préservation.
- Procédure légale : les données en cours d'examen dans le cadre de poursuites en justice (sub judice) peuvent être inaccessibles.

L'adhésion à des codes de conduite professionnels peut faciliter le respect des prescriptions légales.

E. Protection de la propriété intellectuelle

Les dispositifs d'accès aux données devraient tenir compte de l'applicabilité du droit d'auteur ou des autres législations sur la propriété intellectuelle pouvant concerner les bases de données de la recherche financée sur fonds publics. Les facteurs à prendre en compte sont les suivants :

- Compte tenu de la multiplication des partenariats public-privé pour le financement de la recherche et la collecte de données destinées à la recherche, des arrangements équilibrés public-privé devraient faciliter, le cas échéant, un large accès aux données de la recherche. La participation du secteur privé à la collecte des données ne devrait pas, en soi, être une raison pour restreindre l'accès aux données. Il conviendrait de prendre en considération des mesures qui favorisent l'accès et l'exploitation à des fins non commerciales tout en protégeant les intérêts commerciaux, comme la communication différée ou partielle des données ou l'adoption volontaire de mécanismes d'octroi de licences. De telles mesures peuvent permettre aux principaux participants d'exploiter pleinement les données de la recherche, sans en interdire inutilement l'accès.
- Dans les juridictions où les données et informations issues de la recherche publique sont protégées par des droits de propriété intellectuelle, les détenteurs de ces droits devraient néanmoins faciliter l'accès à ces données, en particulier pour la recherche publique ou pour d'autres fins répondant à l'intérêt général.

F. Responsabilité formelle

Les dispositifs d'accès devraient promouvoir des pratiques institutionnelles explicites et formalisées, telles que l'élaboration de règles et de réglementations, sur les responsabilités des diverses parties intervenant dans les activités liées aux données. Ces pratiques devraient concerner la paternité des données, la mention des producteurs, la propriété, la diffusion, les restrictions d'utilisation, les modalités financières, les règles éthiques, les conditions de licence, la responsabilité civile et l'archivage durable.

Les dispositifs d'accès, au niveau gouvernemental comme institutionnel, devraient être élaborés en consultation avec des représentants de tous les acteurs directement concernés. Dans les programmes ou projets de recherche en colla-

boration, et particulièrement dans le cadre de la coopération scientifique internationale ou de projets de recherche fondés sur des partenariats public-privé s'appuyant sur des cadres réglementaires différents, les parties intéressées devraient négocier des accords de partage de données le plus tôt possible au cours du projet de recherche, et dans l'idéal pendant la phase de proposition initiale. On pourra ainsi veiller à ce qu'il soit tenu compte comme il convient et en temps opportun de questions telles que l'allocation de ressources pour le partage et la préservation durable des données de la recherche, les différences dans les législations nationales sur les droits de propriété intellectuelle, les limitations motivées par des considérations de sécurité nationale, ainsi que la protection de la vie privée et de la confidentialité.

Les dispositifs d'accès devraient également prendre en compte des facteurs tels que les caractéristiques des données, leur valeur potentielle pour la recherche, le niveau de traitement des données (données brutes, partiellement traitées ou finales), le fait qu'il s'agisse de données homogènes issues des instruments ou capteurs d'une installation ou de données hétérogènes collectées sur le terrain par des chercheurs isolés, de données sur des sujets humains ou de paramètres physiques, ou encore de données qui sont ou non générées directement par une entité gouvernementale ou grâce à un financement public. Ces variantes dans l'origine ou la nature des données devraient être prises en considération lors de l'établissement des dispositifs d'accès aux données.

De plus, il convient de prendre en compte les éléments suivants :

- Bon nombre de problèmes liés à l'accès, à la diffusion et au partage de données résultent d'un manque d'accords institutionnels explicites sur les modalités d'accès et d'utilisation. La gestion des données devenant toujours plus complexe dans certains domaines de recherche, les arrangements informels conclus traditionnellement entre les chercheurs risquent de ne plus être adaptés et de devoir être complétés par des pratiques et des procédures convenues en bonne et due forme.
- La responsabilité des divers aspects de l'accès aux données et de leur gestion devrait être établie dans les documents concernant les tâches officielles des instituts, les demandes de subventions, les contrats de recherche, les accords de publication et les licences, par exemple.
- La pérennité de l'infrastructure requise pour l'accès aux données revêt une importance particulière. Les établissements de recherche et les organismes publics devraient assumer officiellement la responsabilité de faire en sorte que les données de la recherche soient efficacement préservées, gérées et rendues accessibles de façon à pouvoir être exploitées de manière efficiente et adéquate sur le long terme.

G. Professionnalisme

Les dispositifs institutionnels pour la gestion des données de la recherche devraient être fondés sur les normes professionnelles applicables et sur les valeurs inscrites dans les codes de conduite des milieux scientifiques concernés.

Les facteurs à prendre en compte sont les suivants :

- L'utilisation de codes de conduite/de déontologie par les chercheurs et la communauté scientifique pourrait contribuer à simplifier et à réduire la réglementation régissant l'accès.
- La confiance mutuelle entre les chercheurs, ainsi qu'entre ces derniers et leurs institutions et autres organisations, joue un rôle important dans l'élaboration et le maintien de ces codes de conduite.
- Dans la pratique courante de la recherche, le chercheur ou l'institution qui produit initialement les données est parfois récompensé par l'utilisation exclusive temporaire des données. Les règles applicables à de tels arrangements incitatifs devraient être élaborées et explicitement précisées par les organismes sources de financement, en coopération avec les milieux de la recherche concernés.

Dans certains domaines scientifiques, le manque de préparation et de mise en œuvre de la documentation adéquate et de l'archivage des ensembles de données constitue l'un des obstacles majeurs à l'exploitation maximale de l'investissement dans les données de recherche. Lors de la planification des projets et programmes, à tous les niveaux, les problèmes de données devraient être abordés dès les tout premiers stades afin de prendre en compte les besoins en termes de fonds ou d'assistance technique pour les activités essentielles d'organisation et de conservation de ces ensembles de données. Il conviendrait de prêter attention aux incitations et au développement des compétences professionnelles dans tous les domaines de la gestion des données de recherche.

H. Interopérabilité

L'interopérabilité technologique et sémantique est essentielle pour faciliter et encourager l'accessibilité et l'utilisation des données de la recherche dans un contexte international et interdisciplinaire. Les dispositifs d'accès devraient tenir dûment compte des normes internationales pertinentes applicables en matière de documentation des données. Les pays membres et les établissements de recherche devraient coopérer avec des organisations internationales chargées de l'élaboration de nouvelles normes.

Bien que la science devienne une entreprise fortement mondialisée, l'incompatibilité des normes techniques et procédurales utilisées peut être un obstacle très sérieux aux multiples usages des ensembles de données.

Les facteurs qui devraient notamment être pris en compte sont les suivants :

- Il conviendrait de mentionner explicitement les normes employées dans la mesure où il s'agit de la première exigence de l'interopérabilité.
- Le fait de prendre pour modèle les disciplines les plus avancées à cet égard devrait être encouragé, en particulier par les organisations professionnelles internationales se consacrant à la science ainsi qu'à la collecte et à la conservation des données à des fins scientifiques et technologiques.
- Les travaux d'organisations chargées de définir des normes plus générales concernant les technologies de l'information et des communications devraient également être pris en considération.

I. Qualité

La valeur et l'utilité des données de recherche dépendent pour une large part de la qualité des données elles-mêmes. Les gestionnaires de données et les organisations de collecte de données devraient particulièrement veiller au respect de normes de qualité explicites. Lorsque ces normes n'existent pas encore, les institutions et les associations de recherche devraient, avec leurs chercheurs, se consacrer à leur élaboration. Si tous les domaines de la recherche peuvent tirer parti d'une meilleure qualité des données, certains exigent des normes beaucoup plus rigoureuses que d'autres. Pour cette seule raison, il n'est pas réaliste d'envisager des normes universelles de qualité des données. Les normes devraient être élaborées en consultation avec les chercheurs pour s'assurer que le niveau de qualité et de précision répond aux besoins des différentes disciplines.

Plus spécifiquement,

- Les dispositifs d'accès aux données devraient décrire les pratiques exemplaires quant aux méthodes, techniques et instruments employés pour le recueil, la diffusion et l'archivage accessible des données, afin de permettre un contrôle de qualité par un examen mutuel et d'autres moyens assurant la qualité et l'authenticité.
- L'origine des sources devrait être établie et spécifiée de façon vérifiable. Tous ceux qui souhaitent utiliser les données devraient pouvoir obtenir facilement ces informations, qu'il conviendrait d'incorporer dans les métadonnées accompagnant les ensembles de données. Il est important de constituer ces métadonnées pour permettre aux scientifiques de comprendre les implications exactes des ensembles de données.
- Autant que possible, l'accès aux données devrait être lié à l'accès aux documents de recherche originaux, et les reproductions des ensembles de données devraient être liées aux originaux pour faciliter la validation des données et la détection d'erreurs dans ces ensembles.
- Les établissements de recherche et les associations professionnelles devraient concevoir des pratiques adéquates concernant les références de données et l'enregistrement de ces références sous forme d'index, dans la mesure où ce sont des indicateurs précieux de la qualité des données.

J. Sécurité

Il convient de s'attacher en particulier à encourager l'utilisation de techniques et d'instruments destinés à garantir l'intégrité et la sécurité des données de recherche. En ce qui concerne la garantie de l'intégrité d'un ensemble de données, tout devrait être mis en œuvre pour s'assurer du caractère complet des données et de l'absence d'erreurs. En ce qui concerne la sécurité, les données, de même que les métadonnées et descriptions correspondantes, devraient être protégées contre la perte, la destruction, la modification et l'accès non autorisé, intentionnels ou non, en conformité avec des protocoles de sécurité explicites. Les ensembles de données et les équipements servant à leur conservation devraient également être protégés contre les risques environnementaux tels que chaleur, poussières, surtensions, champs magnétiques et décharges électrostatiques.

K. Efficience

L'un des buts essentiels poursuivis en s'attachant à promouvoir l'accès et le partage des données est d'améliorer l'efficience globale de la recherche scientifique financée sur fonds publics afin d'éviter une duplication inutile et coûteuse des efforts de collecte de données.

Il convient de prendre en compte les aspects suivants :

- Les dispositifs d'accès aux données devraient favoriser l'amélioration du rapport coût-efficacité au sein du système scientifique mondial par la description des pratiques exemplaires dans les services de gestion de données et de soutien spécialisé.
- Si les données de la recherche financée sur fonds publics sont soumises à la règle par défaut d'ouverture énoncée en vertu du Principe A, cela ne signifie pas pour autant que toutes ces données doivent être conservées de manière permanente. Les acteurs de l'archivage de données devraient mener des évaluations coûts-avantages régulières et concevoir et affiner en permanence des protocoles visant à s'assurer que les ensembles de données ayant la plus grande utilité potentielle sont conservés et rendus accessibles. Le recours à des protocoles acceptés de conservation et à une information détaillée sur les données devrait contribuer à réduire les doubles emplois ainsi qu'à établir la sélectivité nécessaire en matière de conservation.
- Des services de soutien spécialisés, par exemple dans le cadre d'une collaboration sur des projets de recherche spécifiques avec des spécialistes hors de la sphère universitaire ou le recours à des organisations spécialisées dans la gestion des données, devraient être envisagés pour veiller à la rentabilité de la production, de l'utilisation, de la gestion et de l'archivage des données de la recherche.
- Si les chercheurs ou les producteurs de bases de données ne bénéficient pas d'incitations suffisantes, ils risquent de relâcher leurs efforts dans les activités liées aux données. Il conviendrait pour éviter ce problème d'envisager l'élaboration de nouvelles structures d'incitations et l'adaptation des structures existantes, notamment la prise en compte des activités de gestion de données dans les procédures de nomination et de promotion.

L. Responsabilité de rendre compte

Le fonctionnement des dispositifs d'accès aux données devrait faire l'objet d'une évaluation périodique par les groupes d'utilisateurs, les institutions responsables et les organismes de financement de la recherche. Même si chaque partie utilisera sans doute des critères d'évaluation quelque peu différents, la somme totale des résultats devrait donner une image détaillée de la valeur des données et des régimes d'accès aux données. Ces évaluations devraient contribuer à accroître le soutien en faveur du libre accès aux données par le milieu scientifique et la collectivité.

Il convient de prendre en compte les aspects suivants pour l'élaboration des critères d'évaluation :

- Les investissements publics globaux dans la production et la gestion des données de la recherche.
- Les performances de gestion des organismes de collecte et d'archivage de données.
- Le degré de réutilisation des ensembles de données existants.
- Les connaissances générées par le réemploi de données existantes.
- Le recours à des exercices de prospective ciblés afin de déterminer la nature et le champ des activités de préservation des données et les catégories de données les plus susceptibles d'être nécessaires à l'avenir.

Même s'il ne sera pas facile de se faire une idée claire et précise des coûts, des avantages et des résultats des dispositifs d'accès aux données, les responsables des dispositifs d'accès aux données devraient s'attacher à montrer les avantages d'un libre accès aux données afin de justifier et d'obtenir un soutien durable de la part de tous les niveaux de gouvernement.

M. Pérennité

Il conviendrait de tenir dûment compte de la pérennité de l'accès aux données de la recherche financée sur fonds publics comme l'un des éléments-clés des infra-structures de recherche. Cela suppose d'assumer la responsabilité administrative des mesures destinées à garantir un accès permanent aux données jugées comme devant être durablement conservées. La tâche peut être difficile étant donné que la plupart des projets de recherche et les financements publics accordés sont de durée limitée, alors que garantir l'accès aux données produites est une entreprise qui s'inscrit dans la durée. Les organismes de financement de la recherche et les établissements de recherche devraient donc étudier la préservation à long terme des données dès le début de chaque nouveau projet, et notamment rechercher les structures d'archivage les plus appropriées pour les données.

Annexe E.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES CONCERNANT LE CONTENU NUMÉRIQUE

Le contenu numérique est devenu un élément de plus en plus important et répandu conditionnant le développement économique et social. Les communications à haut débit, l'augmentation de la bande passante pour les liaisons montantes comme pour les liaisons descendantes, la baisse des tarifs d'accès, la convergence de réseaux auparavant distincts, l'innovation dans les nouveaux équipements terminaux et nouvelles applications et l'abaissement des barrières à l'entrée sont autant de facteurs qui vont induire de nouvelles façons de créer, distribuer et préserver du contenu numérique et d'y accéder. Les économies gagnant en intensité de connaissance, les activités à fort contenu en information auxquelles sont associés la création, la collecte, la gestion, le traitement, le stockage, la distribution et la consultation de contenu se diffusent dans un large éventail d'industries et contribuent au développement de l'innovation, de la croissance et de l'emploi. Le contenu numérique devient essentiel dans la recherche, la santé, l'enseignement et les services sociaux, dans les services liés à la connaissance et la culture et dans l'administration publique. Il stimule également une participation accrue et une offre créative de la part des utilisateurs.

Des politiques appropriées peuvent accroître la contribution du contenu numérique à la croissance et au bien-être et en diffuser plus largement les retombées. La Recommandation du Conseil de l'OCDE de 2004 sur le développement du haut débit[1] a reconnu le rôle croissant du contenu numérique et le Groupe de travail sur l'économie de l'information a entrepris une analyse exhaustive des évolutions et stratégies liées au contenu numérique haut débit et des politiques qui s'y rattachent[2]. Les principes ci-après prennent appui sur ces travaux, sur la conférence sur le thème « L'économie numérique future : création, distribution et accès concernant le contenu numérique » et sur des contributions nationales.

L'objectif de ces principes est d'aider à définir et d'éclairer le contexte du débat politique, et de l'analyse, de l'examen et de l'élaboration des mesures. Des travaux complémentaires seront entrepris par l'OCDE et ses pays membres pour à la fois

1. Voir les travaux sur le suivi de la *Recommandation du Conseil de l'OCDE sur le développement du haut débit*, C(2008)51.

2. Voir les études analytiques à l'adresse www.oecd.org/sti/digitalcontent. Ces études utilisent une approche méthodologique commune pour traiter des défis et questions à venir. Celles-ci couvrent : l'édition scientifique, la musique, les jeux informatiques et vidéos en ligne, le contenu pour mobiles, l'information du secteur public, le contenu créé par l'utilisateur, le cinéma et la vidéo et la publicité en ligne. Une analyse des stratégies et politiques à l'égard du contenu numérique figure dans le document OCDE (2006), *Stratégies et politiques en matière de contenu numérique*, DSTI/ICCP/IE(2005)3/FINAL.

mettre en oeuvre ce cadre, le réviser et l'améliorer à l'avenir[3]. Un large éventail d'acteurs s'intéressent à ces questions. Il est important de les identifier et de les associer aux travaux futurs pour s'assurer de la concrétisation des retombées des innovations liées au contenu numérique et de la large diffusion du contenu, de l'information et du savoir.

Pouvoirs publics et contenu numérique

Il est clairement reconnu que les participants sur le marché créent et développent des modèles économiques pour le contenu numérique, mais les pouvoirs publics ont un rôle dans la mise en place des facteurs qui rendent possibles la création et l'utilisation du contenu numérique, en prenant des mesures qui contribuent à la diversité culturelle, à l'entrepreneuriat lié au contenu local, et en menant une action de facilitation par le développement des possibilités et la suppression des obstacles réglementaires et autres entraves inutiles entre des domaines d'action antérieurement distincts. L'élimination des obstacles à la concurrence dans les services de réseaux, et les politiques qui encouragent l'investissement dans les infrastructures, le contenu et les capacités haut débit dans les zones rurales et isolées et dans les économies en développement jouent un rôle important. Un environnement économique approprié favorable au contenu numérique peut être mis en place en remédiant aux défaillances du marché qui entravent la R-D, l'innovation, l'éducation et la valorisation des compétences. Des conditions cadres non discriminatoires peuvent réduire les obstacles à l'entrée, améliorer les conditions de concurrence et aider à surmonter l'absence de financement. Les pouvoirs publics ont également un rôle important en tant que créateurs et utilisateurs de contenu numérique[4].

Principes relatifs au contenu numérique[5]

Les principes directeurs suivants contribueront à promouvoir un environnement favorable, à renforcer l'infrastructure, et à favoriser un environnement économique et réglementaire propice à la création, à l'accessibilité et à la préservation du contenu numérique.

3. Des travaux complémentaires sont également nécessaires pour mesurer le contenu numérique, élaborer des indicateurs et critères internationaux appropriés et améliorer le recueil, l'étude et l'analyse de données systématiques et comparables.

4. Voir les principes directeurs distincts relatifs à un accès amélioré à l'information du secteur public et son exploitation plus efficace, C(2008)36.

5. Par souci de cohérence, les termes utilisés dans le texte sont ceux de "création, diffusion et préservation de contenu numérique » et d'« utilisation » selon les cas, à moins que le contexte particulier n'impose l'utilisation d'un terme spécifique.

Promouvoir un environnement favorable

- Des politiques qui encouragent un environnement créatif stimulant la création, la diffusion et la préservation de toutes les formes de contenu numérique marchand et non-marchand.
- Des politiques qui facilitent la R-D et l'innovation dans la création, la diffusion et la préservation de contenu numérique, ainsi que les réseaux, logiciels et matériels en relation avec le contenu numérique, les normes ouvertes et l'interopérabilité.
- Des politiques qui aident à faire en sorte que les marchés de capitaux (par exemple capital-risque) fonctionnent de façon compétitive pour financer l'innovation et les activités dans le domaine du contenu numérique.
- Des initiatives visant à répondre aux pénuries en matière de qualifications, de formation, d'enseignement et de valorisation des ressources humaines pour la création, la diffusion et l'utilisation de contenu numérique innovant.
- Des politiques qui stimulent la création de connaissances plus riches et la diffusion, l'utilisation licite et la préservation de différentes formes de contenu numérique (notamment l'accès à l'information, à la recherche, aux données et aux publications), encouragent les investissements dans cette création, diffusion et préservation, et encouragent l'accès planétaire au contenu, quelles qu'en soit la langue et l'origine.
- Des politiques qui améliorent l'accès à l'information du secteur public et permettent qu'elle soit utilisée plus efficacement.
- Créer et assurer un environnement qui encourage la liberté d'expression et l'accès à l'information et aux idées.

Améliorer l'infrastructure

- Des politiques qui encouragent l'investissement dans des infrastructures de réseau, des logiciels, du contenu et des applications de type nouveau.
- Des politiques qui s'attachent à améliorer la parité réglementaire et à assurer un traitement cohérent entre des plateformes de distribution de contenu (notamment les réseaux de prochaine génération), des environnements technologiques et des chaînes de valeur qui diffèrent et dans certains cas convergent.
- Des politiques qui encouragent des approches neutres sur le plan technologique, l'interopérabilité et le développement de normes ouvertes pour répondre aux questions technologiques liées à la création, à la diffusion, à l'utilisation et à la préservation de contenu numérique.
- Des politiques qui améliorent les applications pour la fourniture et l'utilisation du contenu numérique, notamment qui favorisent des outils efficaces de gestion, de préservation et de diffusion propres à améliorer l'accessibilité et l'utilisation des différentes catégories de contenu numérique.

- Des politiques qui favorisent et améliorent l'accessibilité de tous au contenu numérique, quel que soit le lieu, de manière à pleinement concrétiser les retombées de l'économie Internet et de l'environnement numérique mondial.

Promouvoir le climat économique et réglementaire

- Des politiques qui encouragent le développement de modèles économiques d'entreprise innovants, la diffusion des pratiques exemplaires et l'adaptation des chaînes de valeur dans l'environnement numérique.
- Des politiques qui encouragent des cadres politiques et économiques non discriminatoires renforçant la concurrence.
- Des politiques qui reconnaissent les droits et les intérêts des créateurs et des utilisateurs, dans des domaines comme la protection des droits de propriété intellectuelle, tout en encourageant des modèles de cyberactivité innovants.
- Des politiques qui offrent des incitations à la création, la diffusion et la préservation de contenu numérique (par exemple par des stratégies d'innovation ouverte, par une collaboration université-industrie, par la fourniture d'incitations à la recherche à long terme et via les droits de propriété intellectuelle).
- Des politiques qui améliorent la qualité et l'exactitude de l'information et du contenu ; par exemple, des politiques qui facilitent l'utilisation d'outils aidant les créateurs à identifier et diffuser leurs oeuvres et les utilisateurs à identifier des informations et des oeuvres spécifiques et à y avoir accès.
- Des politiques qui renforcent la confiance dans la création et l'utilisation de contenu numérique par un contrôle efficace de l'application des réglementations sur la protection de la vie privée et des consommateurs, en décourageant les déclarations mensongères et vols d'identité et en protégeant les enfants contre les contenus préjudiciables, en informant clairement les utilisateurs des moyens de protection, en réduisant les violations de droits d'auteur sur les produits numériques, oeuvrant pour la sécurité de l'information et des réseaux tout en recherchant l'équilibre entre ouverture et sécurité dans les environnements de contenu, et de façon plus générale en renforçant la coopération transfrontière et les mesures pratiques pour atteindre ces buts.
- Des politiques qui améliorent les transactions commerciales en ligne, notamment des mécanismes pour les paiements et les micropaiements, les signatures et l'authentification électroniques, ainsi que l'interopérabilité internationale de ces mécanismes.
- Clarifier les questions de fiscalité en relation avec les produits de contenu numérique.

Annexe F.
RECOMMANDATION DU CONSEIL RELATIVE À UN ACCÈS ÉLARGI ET UNE EXPLOITATION PLUS EFFICACE CONCERNANT LES INFORMATIONS DU SECTEUR PUBLIC

LE CONSEIL,

Vu l'article 5 b) de la Convention relative à l'Organisation de coopération et de développement économiques en date du 14 décembre 1960 ;

Vu la Recommandation du Conseil concernant l'accès aux données de la recherche financée sur fonds publics [C(2006)184] et la Recommandation du Conseil concernant le développement du haut débit [C(2003)259] ;

Soucieux d'accroître les retours sur les investissements publics dans les informations du secteur public1 ainsi que les retombées économiques et sociales d'un accès, d'une utilisation et d'une réutilisation2 plus larges, du fait notamment d'une distribution plus efficiente, d'une innovation accrue et du développement de nouveaux usages ;

Soucieux de promouvoir une distribution plus efficiente de l'information et des contenus, de même que le développement de nouveaux produits et services d'information, notamment par une concurrence sur le marché entre réutilisateurs de l'information ;

Considérant l'utilité de principes convenus de façon concertée pour un accès élargi et une utilisation plus efficace concernant les informations du secteur public, tant pour le secteur public que pour le secteur privé ;

Reconnaissant que les efforts pour améliorer l'accès aux informations du secteur public et leur utilisation doivent prendre en compte les obligations et restrictions légales, notamment en matière de droits de propriété intellectuelle et de secret commercial, de gestion efficace et sécurisée de l'information à caractère personnel, de confidentialité ainsi que de sécurité nationale, de même que les principes fondamentaux tels ceux de la démocratie, des droits humains et de la liberté de l'information et que, par conséquent, certains principes énoncés dans la présente Recommandation, concernant notamment

1. "Les informations du secteur public" sont définies de façon générale aux fins de la présente Recommandation comme "les informations, y compris les produits et services d'information, générés, créés, rassemblés, traités, préservés, tenus à jour ou financés par ou pour le gouvernement ou des institutions publiques", compte tenu des obligations et restrictions légales visées dans le dernier alinéa du préambule de la présente Recommandation.

2. Sont notamment visés l'utilisation par le producteur ou détenteur initial du secteur public ou par d'autres organismes du secteur public et le réemploi ultérieur par des entreprises ou des particuliers à des fins commerciales ou non. De façon générale, le terme utilisation couvre tout ce large éventail d'utilisations et de réutilisations.

l'ouverture et la réutilisation, peuvent être appliqués à des degrés différents aux diverses catégories d'informations du secteur public.

Sur la proposition du Comité de la politique de l'information, de l'informatique et des communications :

RECOMMANDE que, lorsqu'ils mettent en place ou révisent leurs politiques concernant l'accès aux informations du secteur public et leur utilisation, les pays membres prennent dûment en compte et mettent en oeuvre les principes suivants qui définissent un cadre général pour une utilisation plus large et plus efficace des informations et contenus du secteur public et la création de nouveaux usages à partir de ces sources :

- **Ouverture**. Maximiser la disponibilité des informations du secteur public en vue de leur utilisation et de leur réutilisation en prenant l'ouverture comme règle de base destinée à faciliter l'accès et la réutilisation. Élaborer un régime de principes régissant l'accès ou prendre comme règle de base le caractère ouvert des informations du secteur public chaque fois que possible, quel que soit le modèle de financement de la création et de la tenue à jour de ces informations. Définir les motifs de refus ou de limitation, par exemple pour des raisons de protection de la sécurité nationale ou de la vie privée, ou de préservation d'intérêts privés, s'agissant notamment d'oeuvres protégées par le droit d'auteur, ou en application de la législation, et des règles en matière d'accès national.
- **Accès et conditions transparentes de réutilisation**. Encourager un large accès et des conditions concurrentielles et non discriminatoires pour la réutilisation des informations du secteur public, éliminer les arrangements exclusifs et supprimer les restrictions inutiles sur les modes d'accès, d'utilisation, de réutilisation, de combinaison ou de partage, de telle manière qu'en principe toute l'information accessible soit susceptible d'être réutilisée par tous. Améliorer l'accès à l'information sur Internet et sous forme électronique. Offrir et développer des systèmes d'autorisation automatisés en ligne, dans le cas d'un régime de licences de réutilisation, en tenant compte du principe du droit d'auteur ci-après.
- **Listes de ressources**. Faire mieux connaître les informations du secteur public qui sont accessibles et réutilisables. A cet effet, produire par exemple des listes et inventaires des ressources d'information, de préférence publiés en ligne, et présenter clairement les conditions d'accès et de réutilisation aux points d'accès à l'information.
- **Qualité**. Assurer des pratiques méthodiques de collecte et d'administration des données améliorant la qualité et la fiabilité, notamment par la coopération des divers organismes publics impliqués dans la création, la collecte, le traitement, le stockage et la distribution des informations du secteur public.
- **Intégrité**. Maximiser l'intégrité et la disponibilité de l'information par l'utilisation de pratiques exemplaires dans la gestion de l'information. Élaborer et mettre en oeuvre des mesures de sauvegarde appropriées pour protéger l'information contre des modifications non autorisées ou le blocage intentionnel ou non intentionnel des accès autorisés à l'information.

- **Nouvelles technologies et conservation à long terme**. Améliorer les technologies d'archivage, recherche et extraction interopérables et approfondir les recherches connexes, notamment celles visant à améliorer l'accès aux informations du secteur public et leur disponibilité en plusieurs langues, et veiller au développement des compétences nécessaires dans ce domaine. Traiter le problème de l'obsolescence technologique et relever les défis de la conservation et de l'accès à long terme. Trouver de nouvelles voies pour la numérisation des informations et contenus existants du secteur public, pour le développement de produits et données du secteur public qui soient numériques dès l'origine, et pour les projets de numérisation à caractère culturel (radiodiffuseurs publics, bibliothèques numériques, musées, etc.), dans les cas où les mécanismes du marché n'encouragent pas l'essor de la numérisation.
- **Droit d'auteur**. Les droits de propriété intellectuelle doivent être respectés. Il existe une large gamme d'options pour traiter les droits d'auteur sur les informations du secteur public, depuis la détention des droits par les gouvernements ou des entités privées jusqu'à l'absence de droit sur les informations du secteur public. Exercer le droit d'auteur d'une façon qui facilite la réutilisation (y compris en renonçant aux droits d'auteur et en créant des mécanismes qui facilitent le renoncement aux droits d'auteur quand les titulaires y consentent et en ont la faculté, et en élaborant des mécanismes pour la gestion des oeuvres orphelines) et, le cas échéant, établir en accord avec les détenteurs des droits d'auteur des mécanismes simples pour promouvoir un accès et une utilisation plus larges (y compris des dispositifs simples et efficaces pour la cession de licences) et encourager les organismes publics et autres institutions qui financent des oeuvres de sources extérieures à trouver des moyens de rendre ces oeuvres largement accessibles par le public.
- **Tarification**. Quand les informations du service public ne sont pas fournies gratuitement, veiller à une tarification transparente et cohérente de ces informations à l'intérieur des différentes organisations du secteur public et autant que possible entre elles, afin de faciliter l'accès et la réutilisation et d'assurer la concurrence. Si possible, les frais demandés à l'utilisateur ne devraient pas excéder les coûts marginaux d'entretien et de distribution, et, dans des cas spécifiques, les coûts supplémentaires concernant, par exemple, la numérisation. Fonder toute tarification supérieure aux coûts sur des principes politiques clairement exprimés.
- **Concurrence**. Veiller à ce que les stratégies de tarification prennent en compte les considérations de concurrence déloyale lorsque simultanément des entités publiques et des entreprises privées fournissent des services à valeur ajoutée. Rechercher la neutralité concurrentielle et l'égalité et la rapidité d'accès quand il existe des possibilités de subventions croisées avec d'autres activités publiques qui sont monopolistiques, ou quand les charges sur les activités publiques sont moindres. Imposer aux organismes publics d'appliquer à leurs propres activités en aval/à valeur ajoutée le même traitement qu'à leurs concurrents pour des finalités comparables, notamment sur le plan de la tarification. Prêter une attention particulière aux sources

uniques de ressources d'information. Promouvoir des arrangements non exclusifs pour la diffusion de l'information afin que les informations du secteur public soient ouvertes à tous les utilisateurs et réutilisateurs à des conditions non-exclusives.

- **Mécanismes de recours**. Mettre en place des procédures adéquates et transparentes d'administration des plaintes et de recours.
- **Partenariats public-privé**. Faciliter les partenariats public-privé pour la mise à disposition des informations du secteur public lorsque cela est justifié et praticable, par exemple en trouvant des moyens créatifs de financer les coûts de la numérisation, tout en développant l'accès et les droits de réutilisation par des tiers.
- **Accès et utilisation au niveau international**. Harmoniser davantage les régimes et l'administration de l'accès de manière à faciliter l'utilisation transfrontière, et mettre en oeuvre d'autres mesures pour améliorer l'interopérabilité transfrontière, notamment dans les situations où les utilisateurs non publics sont soumis à des restrictions. Soutenir la coopération et la coordination internationales pour la réutilisation commerciale et l'utilisation non commerciale. Éviter le fractionnement, promouvoir une plus grande interopérabilité et faciliter l'échange et les comparaisons des ensembles de données nationaux et internationaux. Rechercher l'interopérabilité et des formats communs compatibles et largement utilisés.
- **Pratiques exemplaires**. Encourager une large mise en commun des pratiques exemplaires et l'échange d'informations sur les efforts accrus de mise en œuvre, l'éducation des utilisateurs et re-utilisateurs, le renforcement des capacités institutionnelles et les mesures pratiques destinés à promouvoir la réutilisation, sur les modèles de coûts et de tarification, sur le traitement des droits d'auteur et sur le suivi des résultats et le respect des règles, ainsi que sur leurs impacts plus généraux sur l'innovation, l'entrepreneuriat, la croissance et les effets sur la collectivité.

INVITE :

Les pays membres à diffuser la présente Recommandation dans l'ensemble des secteurs public et privé, notamment auprès des gouvernements, entreprises et autres organisations internationales, afin d'encourager tous les participants intéressés à prendre les mesures nécessaires pour étendre l'accès aux informations du secteur public et en promouvoir une utilisation plus efficace.

Les économies non membres à prendre en compte la présente Recommandation et à collaborer avec les pays Membres dans sa mise en oeuvre.

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de promouvoir la mise en oeuvre de la présente Recommandation et de procéder à son réexamen tous les trois ans afin de favoriser un accès élargi aux informations du secteur public et une utilisation plus efficace de ces informations.

Annexe G.
RECOMMANDATION DU CONSEIL SUR LA PROTECTION DES INFRASTRUCTURES D'INFORMATION CRITIQUES

LE CONSEIL

Vu l'article 5(b) de la Convention relative à l'Organisation de coopération et de développement économiques, en date du 14 décembre 1960 ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité [C(2002)131], ci-après dénommée les « Lignes directrices sur la sécurité » ;

Vu la Résolution 58/199 adoptée par l'Assemblée générale des Nations Unies sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information ;

Reconnaissant que le fonctionnement de nos économies et de nos sociétés est de plus en plus tributaire de systèmes et réseaux d'information qui sont interconnectés et interdépendants, au plan tant intérieur qu'international ; qu'un certain nombre de ces systèmes et réseaux sont d'une importance nationale critique ; et que leur protection est un domaine prioritaire pour la politique publique nationale et la coopération internationale ;

Reconnaissant que pour améliorer la protection des infrastructures d'information critiques au plan national et international, les pays Membres doivent partager leurs connaissances et leur expérience dans l'élaboration des politiques et pratiques, et coopérer plus étroitement entre eux, ainsi qu'avec les économies non membres ;

Reconnaissant que la protection des infrastructures d'information critiques nécessite une coordination au plan intérieur et international avec les propriétaires et opérateurs privés de ce type d'infrastructures, ci-après dénommés « le secteur privé » ;

Sur la proposition du Comité de la politique de l'information, de l'informatique et des communications :

CONVIENT que :

Aux fins de la présente Recommandation, les infrastructures d'information critiques, ci-après dénommées « IIC » s'entendent comme désignant les systèmes et réseaux d'information interconnectés, dont la perturbation ou la destruction aurait un sérieux impact sur la santé, la sécurité, la sûreté ou le bien-être économique des citoyens ou sur le fonctionnement efficace du gouvernement ou de l'économie ;

Les IIC sont identifiées par le biais d'un processus d'évaluation des risques et englobent en général un ou plusieurs des éléments suivants :

- Les éléments d'information sur lesquels reposent les infrastructures critiques, et/ou ;
- Les infrastructures d'information sur lesquelles reposent des éléments essentiels des activités gouvernementales ; et/ou
- Les infrastructures d'information essentielles à l'économie nationale ;

RECOMMANDE que :

Les pays Membres mettent en place et maintiennent un cadre efficace pour la mise en oeuvre des Lignes directrices de l'OCDE sur la sécurité en relation avec la protection des IIC, en tenant compte des orientations générales et opérationnelles spécifiques exposées ci-après ;

PARTIE I. Protection des infrastructures d'information critiques au niveau national

Les pays Membres devraient :

Démontrer l'engagement et le soutien des pouvoirs publics en faveur de la protection des IIC en :

- Adoptant au plus haut niveau du gouvernement des objectifs d'action clairs ;
- Identifiant les agences et organisations gouvernementales ayant des responsabilités et des pouvoirs dans la mise en œuvre de ces objectifs d'action ;
- Tenant des consultations avec les propriétaires et opérateurs privés d'IIC en vue d'instaurer une coopération mutuelle pour la mise en oeuvre de ces objectifs ;
- Assurant la transparence sur les délégations de responsabilités aux autorités et agences gouvernementales afin de faciliter une coopération plus étroite au sein des pouvoirs publics et avec le secteur privé ;
- Revoir de façon systématique les cadres politiques et juridiques et les mécanismes d'autorégulation pouvant s'appliquer aux IIC, notamment ceux qui visent à contrer les menaces transfrontières, afin d'évaluer s'il est nécessaire d'améliorer leur mise en oeuvre, de les modifier ou d'élaborer de nouveaux instruments ;
- Prenant des mesures, s'il y a lieu, pour rehausser le niveau de sécurité des éléments des systèmes et réseaux d'information constituant des IIC ;

Gérer les risques à l'égard des ICC en :

- Élaborant une stratégie nationale recueillant l'engagement de tous les intéressés, notamment des plus hauts niveaux du gouvernement et du secteur privé ;
- Prenant en considération les interdépendances;
- Procédant à une évaluation des risques basée sur l'analyse des vulnérabilités et des menaces concernant les IIC, afin de protéger les économies et les sociétés contre les impacts les plus préoccupants au plan national ;
- Élaborant, sur la base d'une évaluation des risques, et en réexaminant régulièrement un processus national de gestion des risques qui précise dans le détail l'organisation, les outils et les mécanismes du suivi nécessaires pour mettre en oeuvre la stratégie de gestion des risques à tous les niveaux, notamment :
  i. La structure organisationnelle appropriée pour fixer des orientations et promouvoir de bonnes pratiques de sécurité au niveau national, et gérer et suivre l'évolution de la situation, de même qu'un ensemble complet de procédures pour assurer l'état de préparation, notamment la prévention,

la protection, l'intervention et le rétablissement de la situation en cas de menaces naturelles ou malveillantes ;

ii. Un système de mesure pour évaluer et jauger les dispositions en place (notamment des exercices et des tests selon les besoins), et permettre la remontée d'informations dans un processus d'actualisation continue ;

- Mettant en place des moyens d'intervention en cas d'incident, tels qu'une équipe de réponse et traitement des incidents informatiques (CERT/ CSIRTs), ayant une mission de surveillance, de veille, d'alerte et de mise en œuvre de mesures de rétablissement de l'IIC, et des mécanismes pour promouvoir la coopération et la communication entre les intervenants chargés de réagir aux incidents ;

Œuvrer en partenariat avec le secteur privé en :

- Établissant des partenariats public-privé de confiance centrés sur la gestion des risques, l'intervention en cas d'incident et le rétablissement de la situation ;
- Permettant des échanges d'information mutuels et réguliers en mettant en place des dispositions de partage de l'information qui prennent en compte son caractère parfois sensible ;
- Encourageant l'innovation par le biais de projets de recherche et de développement public-privé centrés sur l'amélioration de la sécurité des IIC et, le cas échéant, le partage de ces innovations avec d'autres pays ;

PARTIE II. Protection des infrastructures d'information critiques au niveau international

Les pays Membres devraient coopérer entre eux et avec le secteur privé aux niveaux de la stratégie, des politiques et de l'exploitation pour assurer la protection des IIC contre des événements et des circonstances auxquels les pays ne sont pas en mesure de faire face isolément ;

Ils devraient notamment s'engager résolument dans une coopération bilatérale et multilatérale aux niveaux régional et mondial en vue de :

- Partager leurs connaissances et leur expérience en ce qui concerne l'élaboration de politiques et pratiques au plan intérieur et les modèles de coordination avec les propriétaires et opérateurs privés d'infrastructures d'information critiques ;
- Élaborer une compréhension commune :

i. De la gestion des risques applicable aux dépendances et interdépendances transfrontières ;

ii. Des vulnérabilités, menaces et incidences génériques concernant les IIC, afin de faciliter une action concertée contre celles qui ont un caractère généralisé, comme les failles de sécurité et le maliciel, ainsi que pour améliorer les stratégies et politiques de gestion des risques ;

- Rendre disponible l'information sur les agences nationales intervenant dans la protection des IIC et sur leurs rôles et responsabilités, afin de faciliter

l'identification des homologues et améliorer la réactivité de l'action transfrontière ;

- Reconnaître la valeur de la participation aux réseaux internationaux et régionaux de veille, d'alerte et d'intervention sur incident, pour un échange d'information et une coordination robustes au niveau opérationnel, ainsi que pour une meilleure gestion de crise en cas d'incident s'inscrivant dans un contexte transfrontière ;
- Soutenir la collaboration transfrontière pour, et l'échange d'information sur, la recherche et de développement public-privé pour la protection des IIC ;

INVITE :

Les pays Membres à diffuser la présente Recommandation dans l'ensemble des secteurs public et privé, notamment auprès des autorités publiques, des entreprises et des autres organisations internationales afin d'encourager tous les participants concernés à prendre les mesures nécessaires pour la protection des IIC ;

Les économies non membres à prendre en considération la présente Recommandation et à collaborer avec les pays Membres dans sa mise en oeuvre ;

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE de :

Promouvoir la mise en oeuvre de la présente Recommandation et de la réexaminer tous les cinq ans afin d'encourager la coopération internationale sur les questions liées à la protection des IIC.

Annexe H.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES SUR LE VOL D'IDENTITÉ EN LIGNE

I. Introduction

Le problème de l'usurpation (ou vol) d'identité, qui existe depuis toujours, s'est étendu à l'univers virtuel suite au développement de l'Internet et du commerce électronique. Si l'ampleur du phénomène apparaît limitée dans la plupart des pays, ses implications sont cependant considérables dans la mesure où l'usurpation d'identité numérique peut ébranler la confiance des consommateurs dans leur utilisation de l'Internet dans le cadre du commerce électronique. Les gouvernements ont pris des mesures pour lutter contre ce type de fraude – que ce soit en ou hors ligne, au niveau national comme international. Les *Lignes directrices de 1999 de l'OCDE pour la protection du consommateur dans le cadre du commerce électronique* (« les Lignes directrices de 1999 ») et les *Lignes directrices de 2003 de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales frauduleuses et trompeuses* (« les Lignes directrices de 2003 »), comprennent, par exemple, des principes visant à renforcer les cadres institutionnels des pays membres pour lutter contre la fraude commise en et hors ligne. Outre les travaux de l'OCDE, des instruments internationaux tels que la *Convention contre la délinquance en ligne* du Conseil de l'Europe et la *Convention contre le crime organisé trans-national* des Nations Unies ont été développés pour s'attaquer au problème (Appendice H.1).

Les principes énoncés dans les *Lignes directrices* de 1999 et de 2003 forment une base solide pour établir un cadre institutionnel de lutte contre l'usurpation d'identité en ligne et d'autres types de délinquance. L'objet du présent document est de décrire la manière dont les principes présentés dans ces instruments pourraient être étoffés de manière à renforcer et à développer des stratégies effectives dans les pays membres pour combattre l'usurpation d'identité en ligne. Ce document s'intéresse plus particulièrement à la manière dont l'éducation et la sensibilisation des parties prenantes pourraient être améliorées pour mieux lutter contre ce type de délits. Ces orientations s'appuient très largement sur les recherches et analyses contenues dans le *Document exploratoire sur le vol d'identité en ligne* qui a été examiné par le Comité de la politique à l'égard des consommateurs en 2007 (OCDE, 2008).

Définition de l'usurpation d'identité, formes et méthodes

L'usurpation d'identité se produit lorsqu'une personne acquiert, transfère, possède ou utilise sans autorisation des informations personnelles appartenant à une personne physique ou morale, dans l'intention de commettre, ou en relation avec, des actes de fraude ou autres actes de délinquance. Bien que cette définition s'applique aux individus et aux personnes morales, les présentes orientations se limitent aux usurpations d'identité affectant les consommateurs.

Traditionnellement, l'usurpation d'identité consistait à accéder à des données trouvées dans des documents publics ou obtenues à l'occasion d'un vol d'effets personnels, de l'utilisation impropre de bases de données, de carte de crédit, de comptes bancaires ou d'épargne, et à faire un usage frauduleux de ces informations. Comme on le verra plus en détail dans l'Encadré 1 ci-dessous, les accès non autorisés à des données personnelles peuvent être réalisés par différents moyens, qui vont de la fouille de poubelles, au vol de cartes de paiement, en passant par l'invocation de faux prétextes, le coup d'œil par-dessus l'épaule d'une victime, le « skimming », ou le vol de documents comptables.

Encadré 1. Les moyens traditionnels d'accéder à des données personnelles pour le vol d'identité

Pêche dans les poubelles : dans ce cas de figure, les fraudeurs fouillent les poubelles à la recherche de pièces qui y auraient été jetées. C'est de cette manière que les voleurs d'identité obtiennent des copies de chèques de particuliers, de cartes de crédit ou de relevés bancaires, ou d'autres pièces contenant des informations personnelles.

Les prétextes : les « prétexteurs » contactent un établissement financier ou une compagnie de téléphone, en se faisant passer pour un client légitime, et en demandant des informations relatives au compte de ce client. Dans d'autres cas, le « prétexteur » fait partie de l'établissement financier, ou encore ouvre un compte en ligne au nom d'un client.

Le « shoulder surfing » : dans ce cas, le fraudeur regarde par-dessus l'épaule de sa victime ou depuis un point d'observation proche pendant que la victime saisit son code d'identification personnel (« PIN ») à un distributeur automatique de billets.

Le « skimming » : le fraudeur s'empare de données personnelles à partir des bandes magnétiques situées au dos des cartes de crédit ; les données sont alors transmises en un autre lieu ou elles sont ré-encodées pour fabriquer de fausses cartes de crédit.

Le vol de documents comptables : une personne vole des données appartenant à une entreprise (en s'emparant d'ordinateurs ou de fichiers) ou soudoie des personnes internes à l'entreprise pour obtenir ces informations détenues par l'entreprise ou l'organisation.

En ligne, il existe trois grandes méthodes pour obtenir des informations personnelles sur des victimes (voir encadré 2) : *i)* un logiciel conçu pour collecter des informations personnelles est secrètement installé sur un ordinateur ou un autre équipement (fixe ou mobile) appartenant à la victime potentielle (les « maliciels ») ; *ii)* des courriels ou des sites Internet mensongers sont rédigés pour inciter des personnes à révéler des informations personnelles les concernant (hameçonnage ; les courriels d'hameçonnage sont souvent distribués en masse par le biais de pourriels ; de plus en plus, ils vont de pair avec l'installation de maliciels sur les ordinateurs des destinataires.) ; et *iii)* le piratage ou tout autre type d'exploitation d'ordinateurs ou d'appareils mobiles en vue d'obtenir des données personnelles.

Encadré 2. Techniques en ligne pour voler des informations personnelles

Les maliciels : il s'agit d'un terme générique désignant un code ou un programme logiciel injecté dans un système d'informations dans le but de porter atteinte à ce système ou à d'autres systèmes, ou de les subvertir pour des usages autres que ceux prévus par leur propriétaire. On distingue plusieurs sortes de maliciels : les virus, les vers, les chevaux de Troie, les portes dérobées, les enregistreurs de clavier, les gratteurs d'écran, les rootkits, et les logiciels espions (voir les définitions de ces termes dans l'Appendice H.3).

Le pourriel (ou spam) : ce terme renvoie d'habitude aux messages non sollicités, non souhaités et pernicieux (OCDE, 2006c) ; le spam est de plus en plus considéré comme un vecteur de maliciels et d'escroqueries à base d'hameçonnage.

L'hameçonnage : il s'agit d'une tromperie qu'utilisent les voleurs pour « harponner » les informations personnelles d'identification d'internautes trop confiants, et ce au moyen de courriels et de sites Internet miroirs ressemblant à ceux d'entreprises existant véritablement – établissements financiers ou administrations, par exemple. Une attaque par hameçonnage se décomposera généralement comme suit :

- L'hameçonneur envoie à la victime un courriel qui semble provenir d'une société existante car reprenant les couleurs, les graphiques, les logos et la phraséologie de cette société.
- La victime, après avoir lu le courriel, envoie ses informations personnelles au hameçonneur, soit en répondant au courriel soit en remplissant, via un lien hypertexte, un formulaire qui semble provenir de la société en question.
- De cette manière, les informations personnelles de la victime sont transmises directement au fraudeur.

Le piratage : il consiste à exploiter les vulnérabilités de systèmes électroniques ou de certains logiciels afin de siphonner des données personnelles.

Prévalence

L'usurpation d'identité est un problème de plus en plus fréquent qui touche des individus de toutes les classes d'âge et de toutes les catégories sociales. L'encadré 3 donne une description des manières dont les voleurs d'identité abusent des informations personnelles des consommateurs, hors ligne et en ligne. L'usurpation d'identité en ligne a été reconnue comme une source de préoccupation croissante pour les consommateurs depuis quelques années, ayant un impact direct sur les transactions du commerce électronique et mobile (OCDE, 2006c, p. 21). Comme précisé dans l'*Eurobaromètre spécial de l'Union européenne (« UE ») de 2006* (Commission européenne, 2006, p. 12), l'utilisation de l'Internet pour acheter des biens et services en ligne n'est pas encore très répandue puisqu'elle ne concernait en 2005 que 27 % de la population de l'UE, et se limitait pour l'essentiel à des achats nationaux. Une telle limite s'explique en partie par une certaine défiance des consommateurs à l'égard du commerce électronique par crainte que leurs informations personnelles ne leur soient dérobées.[1]

1. En 2006, une enquête en ligne de l'Union Internationale des Télécommunications intitulée *Confiance et sensibilisation dans le domaine de la cybersécurité* (UIT, 2006) concluait que plus de 40 % des internautes ne procèderaient pas à des transactions en ligne pour cette raison.

Encadré 3. Utilisation frauduleuse d'informations personnelles : moyens classiques et techniques en ligne

Utilisation frauduleuse de comptes existants : les voleurs utilisent des comptes existants de leurs victimes : comptes de carte de crédit, comptes chèques, comptes téléphoniques (fixe et mobile), comptes de paiement sur Internet, courriel et autres comptes Internet, comptes d'assurance médicale.

Création de comptes nouveaux : Les voleurs utilisent des informations personnelles de leurs victimes pour ouvrir de nouveaux comptes, qui peuvent être des comptes téléphoniques (fixes et mobiles), des comptes de cartes de crédit, des comptes de crédit, des comptes chèques et comptes d'épargne, des comptes de paiement sur Internet, des comptes d'assurance automobile ou des comptes de paiements médicaux.

Autres actes frauduleux : les fraudeurs peuvent aussi donner à la police les données personnelles de victimes lorsqu'ils sont arrêtés ou accusés d'un acte de délinquance, ou s'en servir pour obtenir un traitement médical, des services, des fournitures, pour louer un logement, pour toucher des prestations sociales, ou dans le cadre de l'emploi.

La lutte contre l'usurpation d'identité

Ces dernières années, plusieurs pays membres ont mis en place des programmes de lutte contre l'usurpation d'identité (voir Appendice H.2). Ces programmes, qui font une large place à l'éducation et la sensibilisation, visent de larges publics : consommateurs, acteurs clés au sein des entreprises, des administrations et des forces de police. Une analyse des difficultés rencontrées fait apparaître que la lutte contre l'usurpation d'identité comporte trois aspects clés :

Prévention – ce que les parties prenantes peuvent faire pour réduire le risque de vol d'identités (améliorer la sécurité de l'identité ; détecter les tentatives et les instances de vol d'identité ; et limiter l'ampleur et la portée des incidents).

Dissuasion – ce que les parties prenantes peuvent faire pour dissuader des individus de se livrer à une usurpation d'identité (sanctions judiciaires, par exemple).

Récupération de l'identité et recours – ce que les parties prenantes peuvent faire pour faciliter la récupération de ce qui a été volé, et les recours des victimes pour les préjudices subis tels que financiers, les atteintes à la réputation ainsi que d'autres préjudices non monétaires.

Les présentes orientations portent principalement sur la prévention contre l'acquisition d'informations personnelles en ligne. La section II présente des idées sur la manière dont les parties prenantes peuvent utiliser l'éducation et la sensibilisation accrue pour *i)* aider les consommateurs à éviter d'être victimes d'usurpation d'identité et *ii)* aider les entreprises et les pouvoirs publics à lutter plus efficacement contre le problème. La section III porte spécifiquement sur les initiatives possibles pour faire connaître aux entreprises les moyens d'améliorer la sécurité des données, et la section IV se penche sur les problèmes liés à l'authentification de l'identité. La section V, enfin, examinera les domaines dans lesquels il serait utile d'approfondir les travaux sur les moyens de lutte contre l'usurpation d'identité en ligne. Si les présentes orientations sont axées sur l'usurpation d'identité en ligne, il convient de noter qu'un grand nombre des mesures suggérées sont également applicables à l'usurpation d'identité hors ligne.

II. Comment l'éducation et la sensibilisation pourraient être améliorées pour prévenir l'usurpation d'identité en ligne

Pour limiter les risques d'usurpation, l'éducation et la sensibilisation des consommateurs, des entreprises, des responsables publics et des médias à ce problème est indispensable. Diminuer ce risque renforcerait la confiance des consommateurs dans le commerce électronique. Comme le stipulent les *Lignes directrices* de 1999, « Les gouvernements, les entreprises et les représentants des consommateurs devraient collaborer en vue d'assurer l'éducation des consommateurs en matière de commerce électronique (…) et de sensibiliser davantage les entreprises et les consommateurs au cadre de protection des consommateurs qui s'applique à leurs activités en ligne » (OCDE, 1999, section VIII). Cette recommandation, laquelle figure également dans les *Principes directeurs de 2003* (OCDE, 2003, section II. F), s'applique directement à l'usurpation d'identité en ligne. L'usurpation d'identité en ligne est une activité frauduleuse de plus en plus complexe, qui utilise des méthodes technologiques sophistiquées en constante évolution. Pour s'y attaquer, une action concertée et coordonnée de toutes les parties prenantes (pouvoirs publics, entreprises et consommateurs) est indispensable. Éducation et sensibilisation sont donc nécessaires pour faire en sorte que les consommateurs, comme les entreprises, aient conscience de l'importance du problème et des formes sans cesse nouvelles qu'il peut prendre.

Structure des programmes d'éducation et de sensibilisation

Pour être efficaces, les programmes d'éducation et de sensibilisation nécessitent *i)* des documents de sensibilisation convaincants et informatifs et *ii)* des institutions et des canaux pour distribuer ces documents et dispenser l'éducation de manière efficace aux parties prenantes. De plus, la coopération et la coordination des initiatives entre parties peuvent donner lieu à des synergies intéressantes et rendre les efforts plus efficaces. L'implication des parties prenantes est donc essentielle en amont dans le cadre de développement des programmes ; les perspectives différentes permettent de mieux déterminer quels sont précisément les besoins en matière d'éducation et de sensibilisation, quels peuvent être les publics cibles et comment les atteindre.

La collecte d'informations pertinentes sur l'usurpation d'identité

La collecte et la diffusion d'informations de base sur la réalité du vol d'identité en ligne sont essentielles pour améliorer la sensibilisation et la connaissance de l'importance du problème et des moyens de le combattre. Cinq types d'information devraient être développés : *i*) des informations statistiques mettant en évidence les développements et les tendances ; *ii*) des informations sur les conséquences non économiques du vol d'identité ; *iii*) des éléments factuels sur les méthodes qu'utilisent les individus pour voler les identités, et *iv*) des recommandations générales pour protéger les identités, et notamment les instruments que peuvent utiliser les consommateurs et les entreprises pour bloquer les intrusions en ligne, et *v*) des recommandations sur les techniques qui permettent d'identifier ou de détecter les tentatives d'usage illicite de données d'identité.

i) Données statistiques mettant en évidence les développements et les tendances

Dans l'établissement et le maintien d'un cadre effectif visant à limiter l'incidence des pratiques frauduleuses contre les consommateurs, les *Lignes directrices* de 2003 appellent les pays membres à prévoir « des mécanismes efficaces pour rechercher, préserver, recueillir et échanger les informations et preuves pertinentes se rapportant à des cas de pratiques commerciales frauduleuses et trompeuses » (OCDE, 2003, section II. A. 2). La compréhension de la portée et de l'ampleur du problème est un élément clé des campagnes d'éducation. Pourtant, jusqu'à présent, l'information concernant l'évolution du phénomène du vol d'identité en ligne n'est en général pas accessible, en dépit de mises en garde dans les pays membres sur la recrudescence de ce phénomène. En outre, lorsque ces données existent, celles-ci rendent rarement compte en détail des formes que peut prendre l'usurpation d'identité en ligne (OCDE, 2008).

Il serait utile que les parties prenantes explorent les moyens d'améliorer l'élaboration d'informations statistiques qui rendent compte de l'évolution du phénomène du vol d'identité. Il serait bon également que ces informations comprennent des données spécifiques sur le vol d'identité en ligne. L'un des indicateurs fréquemment utilisés à cet égard est le nombre de plaintes déposées par des consommateurs. Il serait intéressant de voir quels autres types d'indicateurs pourraient être utiles.

Outre la mesure de l'ampleur du phénomène du vol d'identité, il pourrait être intéressant de déterminer son impact économique sur les individus et sur les pays. Cette information apporterait un éclairage nouveau et illustrerait l'ampleur du phénomène.

Des informations comparables d'un pays à l'autre et entre différentes sources au sein d'un même pays auraient un plus grand impact. Pour ce faire, celles-ci devraient être élaborées, dans la mesure du possible, à partir des efforts de groupes multilatéraux (publics comme privés) qui travaillent dans ce domaine. Des plateformes du secteur privé pourraient être utilisées pour réunir, analyser et diffuser les statistiques concernant l'hameçonnage, le pourriel et les virus à l'échelle mondiale. Parmi ces structures, citons : le Groupe de travail anti-hameçonnage "Anti-Phishing Working Group" (APWG, à www.antiphishing.org), qui travaille à l'élimination de la fraude et du vol d'identité lorsqu'elle passe par l'hameçonnage et par les usurpations d'identité en ligne ; le Groupe de travail "Messaging Anti-Abuse" (MAAWG, à www.maawg.org), dont l'objet est de préserver l'activité de messagerie électronique contre les « exploits » en ligne et les abus tels que l'hameçonnage de messageries, les attaques par maliciels et les autres formes d'abus ; et DigitalPhishNet (DPN, à www.digitalphishnet.org), un forum de collaboration au sein duquel des fournisseurs d'accès Internet, des sites d'enchères en ligne, des établissements financiers et des agents de la force publique mettent en commun leurs statistiques et leurs bonnes pratiques en temps réel pour s'attaquer à l'hameçonnage et aux autres menaces en ligne.

ii) Informations sur les effets indirects de l'usurpation d'identité

Outre ses coûts économiques, l'usurpation d'identité peut avoir d'autres incidences telsque le temps perdu par les victimes pour le rétablissement de leur réputation, les effets négatifs subis par leur réputation, et les difficultés qu'elles

rencontrent par la suite pour rétablir leur crédibilité financière. La collecte d'informations sur ces aspects permettrait de dresser un état des lieux plus complet des implications du vol d'identité, contribuant ainsi à améliorer la sensibilisation.

iii) Éléments factuels sur les méthodes et techniques qu'utilisent les individus pour usurper les identités

L'identification des différentes techniques utilisées pour commettre les vols d'identité est essentielle si l'on veut pratiquer une dissuasion suffisante pour parer efficacement à la menace. Pour être utiles, les informations sur ces techniques doivent être collectées, analysées et actualisées régulièrement afin de suivre l'actualité. Lorsque c'est possible, il serait intéressant que ces informations soient traitées et partagées, non seulement entre les acteurs de la protection du consommateur, mais également avec d'autres organes chargés de l'application de la loi travaillant sur la question du vol d'identité. De fait, le vol d'identité soulève, dans de nombreux cas, des problèmes relevant de la sécurité, de la vie privée et du pourriel (Appendice H.1). Depuis quelques années, les voleurs d'identité font preuve d'une ingéniosité particulièrement impressionnante pour se procurer des informations personnelles. De plus en plus souvent, comme nous l'avons vu précédemment, les logiciels et les pourriels sont associés à l'hameçonnage.

Comme le montre l'encadré 4 ci-dessous, les attaques par hameçonnage sont de plus en plus sophistiquées, prenant des formes diverses et ciblant les appareils fixes comme les mobiles.

Encadré 4. Les variantes de l'hameçonnage

Le pharming : cette méthode, qui utilise les mêmes types d'identifiants usurpés qu'une attaque classique par hameçonnage, redirige les internautes depuis un site Internet authentique (celui d'une banque, par exemple) vers un site Internet frauduleux ressemblant en tout point à l'original. Lorsque le client connecte son ordinateur au serveur de sa banque, une recherche de correspondance du nom de l'hôte est effectuée pour traduire le nom de domaine de la banque (exemple banque.com) sous forme d'une adresse IP. C'est au cours de ce processus que l'adresse IP sera changée.

Le SmiShing : un utilisateur de téléphone mobile reçoit un SMS dans lequel une société confirme son inscription à un service de rencontre et l'informe que ce service lui sera facturé un certain montant par jour mais qu'il peut annuler sa commande en se rendant sur le site Internet de la société. Ce site Internet est évidemment frauduleux et sera utilisé pour voler des informations personnelles.

Le Vishing : dans un courriel frauduleux classique, qui ressemble à s'y méprendre à ceux d'une entreprise ou d'un établissement légitime, l'hameçonneur invite l'internaute à composer un numéro de téléphone. La victime appelle, tombe sur un répondeur automatique qui lui demande des informations personnelles – numéro de compte bancaire ou mot de passe – prétextant « des vérifications de sécurité ». Généralement, les victimes se méfient moins parce qu'elles ne doivent pas transmettre leurs informations personnelles sur un site Internet.

Il convient de noter que toutes les parties prenantes peuvent participer à l'élaboration et au partage des informations sur les méthodes et techniques employées. Pour exploiter au maximum les informations collectées, il est important que des mécanismes soient mis en place pour faciliter le partage des informations de manière efficace.

iv) Informations sur le niveau de sophistication des techniques de vol d'identité en ligne

Il ne suffit pas d'expliquer les différents procédés par lesquels le vol d'identité en ligne peut être commis ; les campagnes d'éducation doivent également alerter les consommateurs sur le fait que ces méthodes sont en perpétuelle évolution. Les messages d'hameçonnage étaient naguère assez naïfs et ne comportaient que du texte. Par exemple, la fameuse « escroquerie 419 » (aussi connue sous le nom de « arnaque nigériane » ou « lettre nigériane » dans sa version de courrier classique) ; les arnaqueurs tentaient de soutirer de l'argent à leurs victimes sous forme de virements bancaires. Généralement ils évoquaient d'importantes sommes d'argent qu'ils promettaient de partager avec leurs victimes si celles-ci les aidaient à les sortir du pays. Les victimes devaient alors avancer divers frais, droits ou taxes, pour permettre le déblocage des fonds. Mais, victime de son succès, cette arnaque est largement connue parmi les internautes et on ne la rencontre plus guère.

Ainsi, devant la nécessité de trouver des systèmes plus complexes, les hameçonneurs ont cherché et trouvé de nouveaux moyens pour obtenir des consommateurs qu'ils leur révèlent leur mot de passe, leurs numéros de comptes bancaires et autres données personnelles. De plus en plus, les systèmes d'hameçonnage utilisent des images et des logos réalisés avec soin imitant ceux d'établissements commerciaux légitimes. Les courriels sont également de plus en plus personnalisés, et peuvent même contenir les premiers chiffres du numéro de la carte de crédit de la cible – qui sont les mêmes dans toutes les cartes de crédit émises par une banque donnée – pour convaincre la victime potentielle que le message provient bien de sa banque. Comme les véritables offres commerciales, les messages d'hameçonnage contiennent de multiples sollicitations invitant la cible à révéler son mot de passe, son âge, son adresse, etc.

Alors que les hameçonneurs utilisaient auparavant des noms de domaine de niveau supérieur tels que « .com », « .biz », ou « .info », ils recourent maintenant à des noms de domaine de petits États insulaires pour éviter d'être détectés ; par exemple « .im » pour l'Île de Man (Royaume-Uni), que les filtres anti-pourriel ne repèrent souvent pas (McAfee, 2006, p. 15). Certains hameçonneurs vont jusqu'à utiliser des certificats auto-signés afin d'utiliser le protocole de sécurité « HTTPS » et de faire apparaître le cadenas de sécurité sur des sites Internet frauduleux.

Pour une meilleure prévention, il est essentiel que les consommateurs et les différentes parties prenantes soient tenus informés des nouveaux stratagèmes et des avatars des dispositifs connus.

v) Recommandations générales pour protéger son identité en ligne

Pour diminuer considérablement le risque de vol d'identité en ligne, voire le prévenir, il peut être utile de fournir aux parties prenantes des recommandations pratiques sur les moyens de protéger leur identité (voir encadré 5). Un certain nombre d'organisations et de gouvernements ont élaboré des séries de recommandations dans ce domaine. L'une des initiatives les plus complètes et les plus ambitieuses est celle du gouvernement des États-Unis, qui a créé un site Internet réunissant des informations sur les moyens de protéger les informations personnelles et d'éviter les escroqueries sur Internet (http://onguardonline.gov), notamment le vol d'identité.

Encadré 5. Hameçonnage : conseils de prévention à l'intention des consommateurs, par OnGuardOnline.gov

- Installer des logiciels anti-virus et anti-logiciels espions, ainsi qu'un pare-feu sur votre appareil fixe ou mobile et veiller à ce qu'ils soient à jour.
- Ne pas cliquer sur les liens contenus dans les messages qui paraissent être du pourriel et ne jamais répondre aux courriels ou aux messages pop-up vous demandant des informations personnelles ou financières. Il faut aussi éviter de couper-coller un lien suspect dans la fenêtre de votre navigateur Internet. Les hameçonneurs peuvent créer des liens qui semblent aboutir à un site donné mais qui en réalité vous mènent sur un site « sosie ».
- Ne jamais communiquer son numéro de carte de crédit ou les numéros de sécurité en réponse à un message qui paraît être du pourriel. Si vous avez des doutes sur l'utilisation de votre compte, contacter l'établissement à l'aide d'un numéro de téléphone dont vous êtes certains de l'authenticité ou ouvrez une nouvelle session de navigateur et saisissez à la main l'adresse Internet correcte de la société.
- Faire suivre tout message d'hameçonnage aux autorités compétentes ou aux groupements professionnels tels que l'APWG, le DPN ou le MAAWG. Les messages d'hameçonnage peuvent également être communiqués à l'adresse spam@uce.gov. Outre les groupements professionnels et autorités compétentes, il peut également être utile d'adresser le courriel d'hameçonnage à l'établissement dont l'identité est usurpée.

Diffusion de l'information

Pour améliorer la prévention, il est essentiel de faire en sorte que les parties prenantes soient conscientes du phénomène de vol d'identité, et qu'elles aient facilement accès à des informations à ce sujet. Il faut à tout le moins que ces informations soient disponibles sur Internet. En outre, il serait utile d'organiser des sessions d'orientation ou de formation dans les établissements scolaires ou au sein de différents groupements. La radio et la télévision constituent également d'excellents vecteurs pour toucher le grand public, de même que les imprimés et les documents sur supports électroniques (CD et DVD). Enfin, les fournisseurs de services Internet et les sites Internet ayant une forte fréquentation comme les outils de recherche et les sites d'enchères, peuvent faire œuvre utile en attirant l'attention des consommateurs sur les informations mises à leur disposition par les gouvernements et les autres parties intéressées.

La coordination des initiatives de formation et de sensibilisation

La coordination des initiatives d'éducation et de sensibilisation est une bonne occasion d'améliorer leur efficacité, allant dans le sens d'une cohérence accrue et d'une simplification des efforts. Cette coordination peut se faire entre les secteurs privé et public et à partir de plateformes locales, nationales et internationales. Cette coordination permettrait de mettre en évidence les pratiques les plus efficaces et d'en étendre l'utilisation. Les fournisseurs de services Internet par exemple, sont extrêmement bien placés pour souligner l'importance du vol d'identité en ligne, et pour orienter leurs abonnés vers des sources d'information.

Il convient de noter que les initiatives de formation et de sensibilisation revêtent plusieurs formes ; au sein des pouvoirs publics, par exemple, la formation des personnes responsables de l'application des lois couvrant le vol d'identité est un

élément important du renforcement de la sensibilisation afin de limiter l'ampleur et la portée du vol d'identité. Un certain nombre de pays sont déjà actifs sur ce front.

Des réseaux internationaux d'autorités de répression tels que le Réseau International de Contrôle et de Protection des Consommateurs (« RICPC ») et le Plan d'Action de Londres pourraient être utilisés comme plateformes pour coordonner et diffuser des informations de sensibilisation à travers les pays membres de l'OCDE (OCDE, 2003, section III. D).

III. La sécurité des données

La sécurité des données doit également être au cœur de toute stratégie visant à lutter contre le vol d'identité. La violation de données peut avoir de nombreuses conséquences préjudiciables ; les consommateurs risquent d'être victimes d'un vol d'identité, l'entité dont le système a fait l'objet d'une effraction est exposée à des poursuites judiciaires pour n'avoir pas protégé les données, et le coût peut être élevé pour toutes les parties touchées. Il faut donc que les pays membres mettent au point et appliquent des normes de sécurité des données (lois et règlements, normes et lignes directrices sectorielles et dispositions contractuelles privées), pouvant aller le cas échéant, jusqu'au lancement d'enquêtes et de poursuites judiciaires contre les entités qui enfreindraient la législation en matière de sécurité des données.

- Les pays membres doivent améliorer la sensibilisation du secteur privé sur la protection des données et inciter les organisations qui collectent et conservent des données sensibles sur les consommateurs à mettre en œuvre des mesures de sécurité concrètes pour protéger les données personnelles de ces consommateurs.

IV. Authentification électronique

L'authentification électronique est reconnue comme un processus utile, qui permet la vérification et la gestion des identités en ligne. Dans les *Orientations pour l'identification électronique* de l'OCDE (2006), dans lesquelles sont énoncés un certain nombre de principes opérationnels visant à aider les pays Membres à établir ou moderniser leurs méthodes d'identification, ce concept s'entend comme une fonction pour établir la validité et l'assurance de l'identité assumée par un utilisateur, un appareil ou un autre type d'entité dans un système d'information ou de communication. Elle peut donc constituer une dissuasion efficace contre le vol ou l'utilisation frauduleuse d'informations personnelles.

La sensibilisation aux bienfaits et aux bonnes utilisations de l'authentification sont des éléments essentiels pour la confiance des utilisateurs en ligne.

Comme le préconise la *Recommandation de l'OCDE sur l'authentification électronique de 2007*, qui invite les pays membres à établir des approches compatibles et non dépendantes des choix de technologie pour permettre l'authentification électronique des personnes physiques et morales à l'intérieur des frontières des pays et entre différents pays, les pays de l'OCDE doivent prendre des mesures pour aider tous les participants à prendre conscience des avantages de l'authentification électronique, aux niveaux tant national qu'international.

L'authentification électronique est actuellement considérée comme l'une des composantes du concept émergent de gestion des identités. Ce système global, dont l'objet serait de permettre aux utilisateurs d'interagir en livrant un minimum d'informations personnelles en ligne, fera l'objet de la plus grande attention par les pays de l'OCDE dans les années à venir.

V. Travaux ultérieurs

Comme nous l'avons vu dès le début de notre étude, trois aspects sont essentiels pour lutter contre le vol d'identité en ligne : *i)* la prévention, *ii)* la dissuasion et *iii)* la récupération de l'identité et les voies de recours. Le présent document s'intéresse principalement sur la prévention, et examine plus précisément les moyens de faire de la pédagogie auprès des consommateurs et des autres parties prenantes pour prévenir le vol d'identité en ligne. Il est toutefois urgent de s'occuper d'autres aspects de ce problème. Le Bureau des Nations Unies sur les Drogues et la Criminalité (UNODC) travaille en concertation avec la Commission des Nations Unies pour le Droit du Commerce International (CNUDCI) à l'élaboration de recommandations de bonnes pratiques pour la prévention, la dissuasion et la récupération des identités volées. La Commission européenne travaille à une définition harmonisée du concept et examine l'opportunité de faire du vol d'identité en ligne un délit pénal spécifique dans toute l'Union européenne. Comme le signale le *Document exploratoire sur le vol d'identité en ligne* (OCDE, 2008), un certain nombre d'agences gouvernementales et d'entreprises privées dans de nombreux pays étudient le problème.

Voici un certain nombre des aspects qui doivent être considérés aux niveaux national et international (par l'OCDE et par d'autres organismes internationaux) :

- Aspects légaux
  - Le vol d'identité doit-il être défini juridiquement en tant que délit spécifique ?
  - Quelles sanctions dissuasives seraient appropriées (amende, confiscation, listes noires, *etc*.) ?
  - Quelles devraient être les voies de recours pour les victimes ?
  - La législation devrait-elle imposer aux entreprises de prendre davantage de mesures pour prévenir les vols d'identité ? Par exemple les entreprises devraient-elles être tenues de signaler les incidents de sécurité susceptibles d'affecter leurs clients lorsque ces incidents peuvent conduire à des vols d'identité, ou bien d'améliorer l'authentification des consommateurs et des clients lorsqu'elles assurent des services ou qu'elles procèdent à des transactions ?

- La coopération transnationale en matière de répression, entre autorités de protection des consommateurs d'une part et entre ces autorités et le secteur privé d'autre part.
  - Comment la coopération transnationale entre autorités de répression peut-elle être renforcée dans les domaines suivants ?

  - Compétences en matière d'investigation et de partage de renseignements avec les autorités étrangères, les entreprises et le secteur privé, et les représentants des consommateurs.
  - Assistance, formation, et soutien aux efforts de répression des autres pays.
  - Mise en œuvre et échange de « bonnes pratiques » en matière d'éducation des consommateurs.

- Récupération de l'identité et recours
  - Quel type d'assistance les pouvoirs publics, les entreprises, et les ONG devraient-elles mettre en place pour aider les consommateurs à rétablir leur identité et à récupérer les sommes perdues et les pertes non monétaires résultant du vol de leur identité ?
  - Des mécanismes de recours doivent-ils être proposés aux consommateurs, et dans l'affirmative, quelles entités doivent être responsables de ces recours ?
  - De quels outils supplémentaires les victimes ont-elles besoin pour s'assurer du rétablissement effectif de leur identité et pour se remettre complètement de l'usurpation de leur identité ?

Appendice H.1 : INSTRUMENTS MULTILATÉRAUX CONCERNANT LE VOL D'IDENTITÉ EN LIGNE

I. Instruments de l'OCDE sur le commerce électronique

OCDE (Organisation de coopération et de développement économiques) (1999), *Les lignes directrices de l'OCDE régissant la protection du consommateur dans le cadre du commerce électronique*, OCDE, Paris, http://www.oecd.org/document/51/0,3343,fr_2649_34267_1824435_1_1_1_1,00.html.

OCDE (2003), *Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, OCDE, Paris, www.oecd.org/sti/consumer-policy .

II. Instruments de l'OCDE concernant la sécurité, la vie privée et le pourriel

Sécurité :

OCDE (2002), *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*, OCDE, Paris, www.oecd.org/dataoecd/16/22/15582260.pdf.

OCDE (2007), *Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique*, OCDE, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

Vie privée :

OCDE (1980), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* OCDE, Paris, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OCDE (2007), *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée*, OCDE, Paris, www.oecd.org/dataoecd/43/28/38770483.pdf.

Pourriel :

OCDE (2006), *Boîte à outils anti-spam et politiques et mesures recommandées*, OCDE, Paris, www.oecd-antispam.org/.

III. Autres instruments internationaux

Conseil de l'Europe (2001), *Convention sur la cybercriminalité,* Budapest, 23 novembre 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Organisation des Nations Unies (2001), *Convention des Nations Unies contre la criminalité transnationale organisée*, 8 janvier 2001, www.unodc.org/pdf/crime/a_res_55/res5525e.pdf.

Appendice H.2 : LES INITIATIVES D'ÉDUCATION EN MATIÈRE DE VOL D'IDENTITÉ DANS LES PAYS DE L'OCDE

Initiatives des pouvoirs publics

États-Unis

En mai 2006, la Federal Trade Commission des États-Unis a lancé l'initiative « Deter, Detect, Defend », une campagne d'éducation qui a pour objet d'aider les consommateurs à prendre les mesures nécessaires pour réduire les risques de vol d'identité, pour contrôler la diffusion de leurs informations personnelles, et pour réagir rapidement lorsqu'ils soupçonnent qu'ils ont été victimes d'un vol d'identité. Cette campagne s'appuie notamment sur un support intitulé *the ID Theft Consumer Education Kit*, et permet aux organisations et aux différents groupements d'informer les consommateurs sur les moyens de réduire les risques de vol d'identité et sur les mesures à prendre lorsqu'on en a été victime. Ce kit se compose des éléments suivants :

- Un fascicule qui fournit des instructions détaillées et les outils pour contribuer à l'éducation des consommateurs.
- Une brochure.
- Un DVD contenant 10 minutes de vidéo – relatant des cas réels et montrant la manière dont les victimes de vol d'identité ont réagi.
- Un CD-ROM contenant tous les supports pédagogiques de manière à permettre une reproduction facile.
- Un guide plus approfondi destiné aux victimes de vol d'identité.

En avril 2007, une Task Force présidentielle spécialisée dans le vol d'identité a publié un rapport dans lequel est présenté un plan stratégique pour faire face aux problèmes posés par le vol d'identité (FTC, Département américain de la justice, 2007a). L'un des principaux axes de ce plan stratégique est d'éduquer les parties prenantes sur les moyens d'empêcher les données sensibles sur les consommateurs de tomber entre les mains de voleurs d'identité. Ce plan stratégique recommande une campagne d'éducation publique sur plusieurs années menée par les autorités fédérales des États et par les autorités locales. Les États-Unis ont aussi créé un site Internet d'information sur la Task Force, permettant de signaler les cas individuels et rappelant les droits des victimes (www.idtheft.gov).

Australie

Le gouvernement australien distribue un kit d'information intitulé, *How to prevent and respond to identity theft* (Comment prévenir le vol d'identité, comment réagir) (www.crimeprevention.gov.au), pour proposer au grand public des stratégies concrètes pour éviter d'être victime d'un vol d'identité. En 2007, il a publié une brochure, *ID Theft : Dealing with identity theft*, à l'occasion de la Semaine sur le vol d'identité de l'Australasian Consumer Taskforce, organisée dans le cadre de la campagne annuelle de sensibilisation à la fraude de la Task Force. Les pouvoirs publics distribuent également une brochure, *E-Crime - A Crime Prevention Kit for Small Business*, qui indique aux petits entrepreneurs les moyens d'éviter d'être victime d'un

acte de délinquance informatique. En juillet 2007, le gouvernement a introduit une série d'initiatives sur la sécurité informatique dans le cadre de l'E-Security National Agenda. Certaines de ces initiatives ont pour but d'améliorer la sensibilisation aux problèmes de sécurité informatique chez les particuliers et dans les petites entreprises et de généraliser le programme national et international d'exercice sur la sécurité informatique. Le site Internet du gouvernement consacré à la sécurité informatique, *Stay Smart Online* (www.staysmartonline.gov.au), donne aux internautes des conseils pratiques pour sécuriser un ordinateur personnel, effectuer des transactions en ligne, ainsi que des informations pour protéger les enfants et les jeunes sur l'Internet. Le groupe océanien (Australie et Nouvelle-Zélande) Australasian Consumer Fraud Taskforce a créé *ScamWatch* (www.scamwatch.gov.au), un site d'informations sur la fraude sur Internet destiné aux consommateurs et qui leur présente les différents types d'escroquerie, de systèmes et de fraudes. Il contient aussi un dispositif permettant de déclarer les cas de fraude.

Canada

Le Comité des mesures en matière de consommation (CMC), organisation qui représente les ministères fédéraux, provinciaux et territoriaux chargés de la consommation, a élaboré un kit d'information pour aider les consommateurs à se prémunir contre le vol d'identité et leur indiquer les procédures à engager s'ils en sont victimes. De plus, le CMC a préparé un document d'orientation à l'intention des entreprises, contenant des conseils pour protéger les informations personnelles de leurs clients (voir www.cmcweb.ca/idtheft). Un certain nombre d'autres initiatives en cours ont pour objet d'informer les consommateurs sur le vol d'identité en ligne. Citons le Forum de prévention de la fraude, qui regroupe des administrations, des autorités judiciaires et des représentants du secteur privé, qui organise le *Mois de sensibilisation à la fraude* tous les ans en mars, avec pour slogan *La fraude : Identifiez-la. Signalez-la. Enrayez-la.* Le vol d'identité, qui est une forme de fraude parmi d'autres, représente une part importante des informations présentées au public pendant le *Mois de sensibilisation à la fraude*.

Royaume-Uni

Au Royaume-Uni, le Comité directeur sur le vol d'identité au sein du Home Office a lancé un site Internet www.identity-theft.org.uk qui contient aussi des recommandations pour éviter les vols d'identité. En outre, le Bureau du Commissaire de l'Information a produit des supports pédagogiques sur le vol d'identité dans le cadre d'une boîte à outils d'information ; des spots télévisés ; un DVD de formation.

Mexique

Au Mexique, l'Université nationale autonome du Mexique (UNAM) (publique) a mis en place un certain nombre de sites Internet pour alerter les consommateurs et les internautes sur tous les risques qui pèsent sur la sécurité en ligne. Les internautes peuvent y puiser des conseils pour repérer les arnaques (www.seguridad.unam.mx/doc?ap=articulo&id=121), le pharming (www.seguridad.unam.mx/usuario-casero/pharming.dsc), le phishing (www.seguridad.unam.mx/usuario-casero/phishing.dsc) et des trucs pour empêcher le piratage et les atteintes à la sécurité (www.seguridad.unam.mx/doc?ap=articulo&id=118).

Belgique

En Belgique, plusieurs campagnes sont en cours sur la sensibilisation aux risques Internet, dont fait partie le vol d'identité. Tous les supports sont utilisés : guides (Guide pour l'internaute), sites Internet (www.saferinternet.be, qui s'adresse aux enfants, http://economie.fgov.be du Service public fédéral Économie, qui contient des informations sur les droits des consommateurs en droit belge), communiqués de presse sur la fraude Internet destinés à attirer l'attention des consommateurs sur les pratiques frauduleuses sur l'Internet comme le phishing.

Japon

Au Japon, le Ministère des affaires intérieures et des télécommunications (MIC) a lancé un site Internet intitulé *Informations sur la sécurité à l'intention de l'ensemble des internautes* (www.soumu.go.jp/joho_tsusin/security/index.htm) qui contient des informations de base sur la sécurité des données et sur les mesures préventives de lutte contre les menaces en ligne telles que le vol d'identité.

Initiatives du secteur privé

Dans certains pays membres, le secteur privé participe également à des initiatives d'éducation.

Royaume-Uni

Au Royaume-Uni, un certain nombre d'associations de banques et de systèmes de paiement, telles que le British Banker Association (BBA) et le UK payments Association (APACS), se sont montrées particulièrement actives en menant des initiatives de sensibilisation auprès de leurs propres membres (banques et sociétés) comme de leurs clients ; on trouvera plus d'informations sur l'Internet sur le site *www.banksafeonline.org.uk* (OFCOM, 2006, p. 37).

Pays-Bas

Aux Pays-Bas, le *Nederlands Vereniging van Banken*, l'Association des banques néerlandaises, a lancé une campagne de sensibilisation en 2006 pour informer les consommateurs des risques de vol d'identité et pour leur expliquer les moyens de protéger leurs informations personnelles (INTERVICT, 2006, p. 24).

États-Unis

Aux États-Unis, un certain nombre de secteurs d'activité s'intéressent activement aux initiatives éducatives pour lutter contre le vol d'identité. Les établissements financiers, par exemple, qui peuvent être les principales victimes des attaques par hameçonnage, sont de plus en plus nombreux à alerter leurs clients sur les nouveaux messages d'hameçonnage et les nouveaux risques qui pèsent sur la sécurité. Depuis 2004, les établissements financiers ont entrepris une action conjointe de sensibilisation par l'intermédiaire du Centre d'assistance sur le vol d'identité (Identity Theft Assistance Center), organisation nationale représentant certaines des plus grands banques des États-Unis ainsi que des agents de change et des sociétés financières. En outre, l'Association nationale des courtiers en valeurs mobilières a publié un guide intitulé « Phishing et autres types d'escroquerie basés sur le vol d'identité en ligne : ne

mordez pas à l'hameçon ». Plus récemment, le groupe Identity Theft Prevention and Identity Management Standards Panel (IDSP), créé sous l'égide du Better Business Bureau (BBB) et de l'American National Standards Institute (ANSI) a lancé une nouvelle initiative portant sur l'ensemble du marché, dont l'objet est de contribuer à doter les entreprises et les autres entités des outils nécessaires pour lutter contre le vol d'identité en ligne et la fraude, et de protéger les consommateurs (et de se protéger elles-mêmes) contre les risques associés à ce type de délits : www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3. Ce rapport contient un catalogue des standards existants, des bonnes pratiques et des dispositifs d'application relatifs à cette question dans l'ensemble des secteurs et des activités, ainsi que des recommandations sur les autres domaines dans lesquels les pouvoirs publics et le secteur privé devraient élaborer des standards et des orientations. Il donne également un certain nombre de recommandations pour les initiatives de sensibilisation des consommateurs à des parades telles que le blocage des nouveaux crédits.

Australie

En Australie, l'Australian Bankers Association (ABA), l'Australian High Tech Crime Centre et l'Australian Securities and Investments Commission (ASIC), gèrent conjointement un site, *Protégez votre identité financière* (www.protectfinancialid.org.au) qui aide les individus à protéger leur identité financière et à limiter les dégâts si un problème survient. Il contient des conseils pratiques de prévention, des fiches d'information et un test interactif qui permet à chacun d'évaluer le niveau de sécurité de ses données personnelles.

Mexique

Au Mexique, quelques membres de l'Association de l'Internet mexicain (AMIPCI) ont créé un site Internet (consultable à l'adresse www.navegaprotegido.com.mx), qui contient des informations pour aider les consommateurs à mieux comprendre les risques liés au vol d'identité.

Coordination des initiatives d'éducation

États-Unis

Aux États-Unis par exemple, les services du Procureur général assistent à des séminaires de formation et un certain nombre d'organismes chargés du respect de la loi – parmi lesquels le Département de la justice des États-Unis, le Secret Service, la FTC, et le FBI – de même que la American Association of Motor Vehicle Administrators ont conjointement organisé plus de 20 séminaires de formation d'une journée sur le vol d'identité à l'intention des autorités des États et des autorités locales de police du pays (US FTC, 2007a, Vol. II, p. 71 à 73).

Australie

En Australie et en Nouvelle-Zélande, le groupe Australasian Consumer Fraud Taskforce soutient une démarche coordonnée de sensibilisation et d'éducation. Ce groupe, formé en mars 2005, rassemble 18 agences de régulation et bureaux chargés de la protection du consommateur contre les escroqueries et les arnaques. Dans ses

efforts d'amélioration de la sensibilisation aux risques d'arnaques, cette Taskforce a également pour partenaires un large éventail d'organisations communautaires, non gouvernementales et représentatives du secteur privé.

L'objet de la Taskforce est de favoriser la collaboration des pouvoirs publics pour :

- Donner plus d'efficacité aux efforts de répression de l'escroquerie et des arnaques menés par les autorités d'Australie et de Nouvelle-Zélande.
- Organiser une campagne annuelle coordonnée d'information des consommateurs : le *Mois de sensibilisation à la fraude* en février ou mars (pour coïncider avec le Mois de prévention de la fraude dans le monde).
- Inviter les entreprises à participer à la campagne d'information et les encourager à partager les informations qu'elles peuvent avoir sur les fraudes et les escroqueries.
- Susciter davantage d'intérêt pour la recherche sur les fraudes et les escroqueries touchant les consommateurs.

Mexique

Au Mexique, le groupe de travail eCrime, constitué d'entités publiques et privées, parmi lesquelles l'Association des banques mexicaines (ABM), la Chambre nationale des industries de transformation (Canacintra), la Banque nationale du Mexique (Banamex), la banque Bancomer, l'Association Internet du Mexique (AMIPCI), la police fédérale de prévention, la Commission fédérale des télécommunications (COFETEL), la Banque nationale du Mexique, la Commission nationale des banques et des marchés financiers (CNBV), Nic Mexico et l'Université publique UNAM, a été créé pour réunir des données sur le phénomène du phishing et pour neutraliser les noms de domaine associés à des usurpations d'identité.

Belgique

En Belgique, le Service public fédéral Économie, PME, travailleurs indépendants et énergie (FPS Économie), la Federal Computer Crime Unit (FCCU) et le Centre de recherche et d'information des organisations de consommateurs (CRIOC) organisent plusieurs campagnes d'information portant notamment sur le vol d'identité. Par exemple, la campagne de prévention de la fraude 2006 « Arnaqué, moi ? jamais ! » a été organisée sous l'égide de l'International Consumer Protection and Enforcement Network (ICPEN), avec un ciblage spécifique sur l'usurpation d'identité et la fraude contre les consommateurs dans le cadre des services téléphoniques et la fraude liée à la consommation sur l'Internet. La diffusion emprunte plusieurs canaux : prospectus adressés par courrier ou distribués par les services sociaux des grandes villes et à la boutique d'information du FPS Économie (http://mineco.fgov.be/protection_consumer/fraud_prevention/home_fr_001.htm); spots radiodiffusés ; conférences de presse et publications dans des lettres d'information de partenaires externes et dans la presse ; en-tête des relevés de carte de crédit et des factures de téléphone. Cette campagne est financée par le FPS Économie et réalisée avec le soutien de partenaires externes (Belgacom, Loterie nationale, Proximus, Mobistar, Base, Diners Club, Citibank, American Express, Europabank, Les Maisons de justice, etc.).

Appendice H.3 : TERMINOLOGIE

- *Les enregistreurs (mouchards) de clavier* : un enregistreur de clavier est un logiciel qui détecte et enregistre les touches frappées sur un clavier. Il existe deux types d'enregistreur de clavier : ceux qui nécessitent que l'attaquant récupère les données enregistrées sur le système compromis et ceux qui transmettent activement les données enregistrées.
- *Les rootkits* : un rootkit est un ensemble de programmes conçus pour masquer les atteintes faites à l'intégrité d'un logiciel au niveau le plus privilégié ou « root ». Comme la plupart des maliciels, les rootkits ont besoin d'un accès d'administrateur pour bien fonctionner ; une fois installés ils peuvent être quasiment indétectables.
- *Le pourriel* : il semble qu'il y ait une corrélation de plus en plus forte entre les maliciels, l'hameçonnage, et le pourriel. Le terme de pourriel (en anglais spam) couvre généralement les messages électroniques non sollicités, non souhaités et pernicieux.
- *Les chevaux de Troie* : un cheval de Troie est un logiciel informatique qui n'éveille pas les soupçons mais qui en réalité effectue des actions masquées pour contourner les mesures de sécurité et ouvrir la voie à des attaques. Généralement, un cheval de Troie pénètre dans le système d'un internaute en exploitant une vulnérabilité du navigateur ou une de ses fonctions.
- *Les virus* : un virus est un logiciel caché qui s'étend en infectant un autre programme et en insérant dans ce programme une copie de lui-même. Un virus a besoin d'un programme hôte pour fonctionner avant de devenir actif. Le terme de « virus » s'utilise de plus en plus au sens large pour décrire les virus et les vers.

BIBLIOGRAPHIE

ANSI (American National Standards Institute) et BBB (Better Business Bureau) (2008) Rapport final du panel ANSI-BBB « Identity Theft Prevention and Identity Management Standards « , 31 janvier 2008, www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3.

BWGCBMMF (2004), *Rapport sur le vol d'identité*. Rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis, Octobre 2004, http://www.ps-sp.gc.ca/prg/le/bs/report-fr.asp.

CE (Commission européenne) (2006), DG SANCO, Eurobaromètre spécial «Consumer protection in the Internal Market», septembre 2006, Bruxelles, http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf.

FTC (Federal Trade Commission) et Département de la Justice (États-Unis) (2007a), Combating Identity Theft: A Strategic Plan (Lutte contre le vol d'identité : un plan stratégique), US Identity Theft Task Force du Président, 23 avril 2007, www.idtheft.gov.

FTC (2007b), Report on *Consumer Fraud and Identity Theft Complaint Data* (Rapport sur la fraude contre les consommateurs et les données concernant les plaintes pour vole d'identité), www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

INTERVICT (International Victimology Institute Tilburg) (2006), Le défi de la lutte contre le vol d'identité, Rapport commandé par le Programme national néerlandais sur la cyberdélinquance contre les infrastructures ("NICC"), 6 septembre 2006, www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf.

McAfee (2006), *Rapport sur la délinquance virtuelle*, décembre 2006, www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

OCDE (Organisation de coopération et de développement économiques) (1999), *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*, OCDE, Paris, http://www.oecd.org/dataoecd/17/59/34023530.pdf.

OCDE (2003), *Les lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, OCDE, Paris, http://www.oecd.org/dataoecd/24/33/2956464.pdf.

OCDE (2006a), *Rapport sur la mise en œuvre des Lignes Directrices de 2003 sur la Fraude Transfrontière*, OCDE, Paris, http://www.oecd.org/dataoecd/2/5/37133090.pdf.

OCDE (2006b), *Le commerce mobile*, DSTI/CP(2006)7/FINAL, Direction de la Science, de la Technologie et de l'Industrie, www.oecd.org/sti/consumer-policy.

OCDE (2006c), *Boîte à outils anti-spam: politiques et pratiques recommandées*, OCDE, Paris, http://www.oecd-antispam.org/sommaire.fr.php3.

OCDE (2007), *Recommandation sur le règlement des litiges de consommation et leur réparation*, OCDE, Paris, http://www.oecd.org/document/4/0,3343,fr_2649_201185_38960324_1_1_1_1,00.html.

OCDE (2008), *Document exploratoire sur le vol d'identité en ligne,* DSTI/CP(2007)3/FINAL, Direction de la Science, de la Technologie et de l'Industrie.

OFCOM (Office of Communications) (Royaume-Uni) (2006), *Protection en ligne : Enquête sur les consommateurs, les entreprises, et les systèmes et mécanismes de régulation*, 21 juin 2006, www.ofcom.org.uk/research/technology/onlineprotection/report.pdf.

UIT (Union Internationale des Télécommunications) (2006), *Enquête sur la confiance et la sensibilisation dans le domaine de la cybersécurité*, résultats au 17 mai 2006, www.itu.int/newsroom/wtd/2006/survey/charts/q_8.asp.

Annexe I.
ORIENTATIONS DE L'OCDE POUR LES POLITIQUES CONCERNANT LES QUESTIONS ÉMERGENTES DE PROTECTION ET AUTONOMISATION DES CONSOMMATEURS DANS LE COMMERCE MOBILE

I. Introduction

Évolutions du commerce mobile

Dans le présent document, l'expression commerce mobile, ou « commerce électronique mobile » désigne les transactions commerciales et activités de communication conduites par le biais de services et réseaux de communication hertziens au moyen de messages texte (ou SMS - short message service), de messages multimédia (MMS – multimedia messaging service), ou de l'Internet, sur de petits terminaux mobiles de poche, en général utilisés pour les communications téléphoniques. De même, l'expression « opérateur mobile » désigne toute entreprise offrant des services à des abonnés mobiles ; une « entreprise de commerce mobile » désigne une entreprise vendant des biens et des services par l'intermédiaire de plateformes mobiles, soit directement soit via des intermédiaires, y compris les opérateurs de sites Internet (comme Yahoo!, eBay, etc.) et les agrégateurs mobiles (c'est-à-dire des entités qui assistent les entreprises de commerce mobile par exemple en traitant les factures émises par les différents entreprises de commerce tierces et en les transmettant aux opérateurs mobiles pour facturation des abonnés mobiles) ; un « abonné mobile » désigne une personne acquittant un abonnement de téléphonie mobile.

Avec la convergence des plateformes d'exploitation, le commerce mobile s'étend au commerce électronique sur Internet. De ce fait, il est de plus en plus difficile de distinguer le commerce mobile des autres formes de commerce électronique. Bien que le commerce mobile ne nécessite pas en soi un accès à Internet, le nombre de transactions de commerce mobile augmente sans cesse via les protocoles de systèmes de télécommunication [comme le Web (HTML, TPC/IP), le WAP (Wireless Application Protocol) et l'i-mode] et des téléphones portables reliés à des réseaux de communication sans fil (« 3G »). De plus, un nombre croissant d'assistants numériques personnels (PDA) ou de téléphones multifonctions peuvent utiliser les réseaux de communications téléphoniques sans fil.

Le commerce mobile se développe actuellement à un rythme rapide dans de nombreux pays membres de l'OCDE. Dans ces pays, de plus en plus de personnes disposent de téléphones portables évolués ou d'autres équipements analogues qui leur permettent de bénéficier d'un large éventail de services mobiles différents de ceux actuellement utilisables depuis des ordinateurs fixes. Entre 1997 et 2005, le nombre d'abonnés mobiles dans la zone de l'OCDE a progressé à un taux annuel composé moyen de 24 % (OCDE, 2007b, p. 98).

Actuellement, les abonnés à la téléphonie mobile peuvent utiliser leurs terminaux :

- Pour acheter et télécharger des contenus, tels que films, musiques, sonneries ou jeux.
- Pour jouer en ligne à des jeux vidéos ou des jeux d'argent.
- Pour accéder à des informations consultables sur un écran de portable, comme des prévisions météorologiques ou des informations de presse, ainsi qu'à des programmes de télévision mobile ou des programmes d'information en relation avec les programmes, couplés aux canaux de télévision.
- Pour obtenir des informations personnalisées en fonction de leur localisation grâce à des technologies de positionnement (géolocalisation).
- Pour accéder à des services bancaires ou financiers en ligne, et effectuer des transactions.
- Pour effectuer le paiement d'activités sur mobile, dont le montant est prélevé soit sur une carte de crédit soit sur la facture du téléphone portable.
- Comme moyen de paiement (porte-monnaie électronique) pour acheter des biens ou des services ; et
- Pour voter à l'occasion de programmes de télévision interactifs.

Le développement de services mobiles de troisième génération (3G), donnant un accès à l'Internet haut débit sur téléphone portable, pour des communications enrichies par du son et des graphiques de haute qualité, a renforcé l'intérêt des consommateurs pour ces équipements et ouvert la possibilité de nouvelles applications commerciales.

Une autre évolution est le développement de l'accès et de l'utilisation des téléphones portables par les enfants. Faire en sorte que les enfants puissent bénéficier des opportunités offertes par les équipements mobiles tout en bénéficiant d'une protection efficace contre des pratiques et des offres de marketing mobile agressives inappropriées et abusives est un enjeu majeur pour tous les acteurs.

Nouveaux défis pour les consommateurs induits par le commerce mobile

Le Comité de la politique à l'égard des consommateurs (CPC) suit les évolutions du commerce mobile depuis un certain nombre d'années. En 2007, le Comité a publié un rapport (OCDE, 2007a) présentant un tour d'horizon du commerce mobile et identifiant certains des principaux défis qu'il allait présenter pour les consommateurs. Le rapport note que les terminaux mobiles présentent des spécificités uniques qui suscitent l'intérêt des consommateurs (commodité d'emploi et accessibilité permanente aux services souhaités partout où le service mobile est disponible), mais que ceux-ci présentent également des contraintes techniques propres, du fait de limitations dans la taille de l'écran, dans la capacité de stockage et de mémoire, dans l'autonomie et dans la puissance de traitement.

L'idée est ici de proposer un certain nombre de mesures pratiques que les acteurs pourraient adopter pour faire face à plusieurs problèmes apparus dans des pays où le marché est bien développé. Mais d'autres problèmes pourraient aussi se présenter dans l'avenir. Il ne s'agit donc pas de proposer un ensemble complet de principes d'orientation et de mesures, mais plutôt de proposer quelques principes pour guider une exploration et une analyse évolutives des défis actuels et futurs

présentés par le commerce mobile. Ces défis sont présentés ci-après sous la forme d'exemples théoriques.

Le Comité a décidé de se concentrer sur trois questions :

- Les problèmes que pourrait poser le fait que sur les équipements mobiles les possibilités de présentation d'informations sont limitées (en raison de la petite taille de l'écran et d'autres limitations techniques).
- Les risques accrus d'exploitation commerciale des mineurs ; et
- La vulnérabilité accrue des équipements mobiles en ce qui concerne les accès non autorisés, la sécurité des données, les intrusions et la vie privée.

Le Comité a décidé d'examiner ces questions en se référant aux *Lignes directrices de l'OCDE de 1999 régissant la protection des consommateurs dans le contexte du commerce électronique* (« *Lignes directrices sur le commerce électronique* ») (OCDE, 1999). Bien que la plupart des délégations aient considéré que les principes contenus dans les *Lignes directrices sur le commerce électronique* s'appliquent au commerce mobile, elles ont reconnu qu'il serait intéressant de préciser la façon dont ces principes pourraient être efficacement appliqués aux opérateurs mobiles, aux opérateurs de sites Internet, aux agrégateurs mobiles et aux entreprises de commerce mobile vendant des services financiers et autres services commerciaux, ainsi qu'aux abonnés mobiles, pour répondre aux questions évoquées ci-dessus. Dans ce contexte, le Comité intègrerait également certaines pratiques exemplaires issues d'autres instruments pertinents de l'OCDE relatifs à la protection du consommateur, la sécurité, la vie privée et le spam (voir la liste dans l'appendice I.2).

II. Restriction de l'information

Les *Lignes directrices sur le commerce électronique* indiquent que les consommateurs devraient avoir à leur disposition, avant de contracter, des informations leur permettant de prendre des décisions en connaissance de cause dans leurs transactions électroniques. Ces informations, qui devraient être exactes et facilement accessibles à tout moment, sont les suivantes (Encadré 1) :

- Des informations sur l'entreprise et sur les mécanismes de résolution des litiges disponibles.
- Les caractéristiques des biens ou services proposés ; et
- Des détails sur la transaction elle-même, notamment les termes, conditions et modalités de paiement, ainsi que sur les coûts.

Encadré 1. Principales dispositions relatives à l'information dans les *Lignes directrices sur le commerce électronique*

La Partie II des *Lignes directrices sur le commerce électronique* expose les principes généraux suivants :

- La Section II (« Loyauté des pratiques en matière de commerce, de publicité et de marketing") énonce plusieurs principes généraux précisant que les entreprises ne devraient pas s'engager dans des pratiques susceptibles d'être mensongères, trompeuses, frauduleuses ou déloyales ; que les entreprises qui assurent la vente, la promotion ou le marketing de biens ou de services auprès des consommateurs ne devraient pas s'engager dans des pratiques de nature à entraîner un risque excessif de préjudices pour les consommateurs ; et que les entreprises devraient présenter les informations sur elles-mêmes et sur les biens et services qu'elles proposent de façon claire, visible, exacte et facilement accessible.
- La partie C de la Section III (« Informations en ligne – informations sur la transaction ») précise que les entreprises devraient fournir des informations suffisantes sur les modalités, les conditions et les coûts associés à la transaction pour permettre aux consommateurs de décider en toute connaissance de cause de s'engager ou non dans la transaction. Ces informations doivent être claires, exactes et facilement accessibles et comprendre le détail de l'ensemble des coûts perçus et/ou imposés par l'entreprise.
- La Section IV (« Processus de confirmation ») indique que le consommateur devrait pouvoir, avant de conclure l'achat, passer en revue les détails de celui-ci et exprimer son consentement exprès, éclairé et délibéré pour compléter la transaction. Elle indique également que le consommateur devrait pouvoir conserver une trace complète et exacte de la transaction. Enfin, celui-ci devrait pouvoir mettre un terme à la transaction avant de conclure l'achat.
- La Section VI (« Règlement des litiges et recours ») encourage les entreprises à offrir aux consommateurs des mécanismes équitables, efficaces, transparents et internes pour le traitement des plaintes. A cet égard, la Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation invite le secteur privé à mettre en place des « procédures efficaces de traitement de recours internes, offrant aux consommateurs la possibilité de régler leurs litiges directement avec l'entreprise concernée d'une manière équitable, efficace et rapide, sans imposer de frais ou charges pour pouvoir accéder à ou utiliser ces procédures ».

La fourniture d'informations aussi complètes aux consommateurs est complexe s'agissant du commerce électronique, du fait des contraintes techniques propres aux équipements mobiles telles que la petite taille de l'écran ou, sur de nombreux terminaux, la limitation de la mémoire ou de la capacité de stockage. Les offres de services ou de biens sur les téléphones portables prennent en général la forme de SMS ou message électronique. De plus, ces offres peuvent être proposées sur des sites Internet, consultables par portable. Avec la multiplication des équipements mobiles donnant accès à l'Internet, même si les obligations en matière d'information peuvent être formellement satisfaites, il se pourrait que pour des raisons techniques, l'information ne soit pas suffisamment accessible aux utilisateurs de la téléphonie mobile.

Accès à l'information sur les entreprises, les biens et services et le processus de transaction

Offre d'un téléviseur

Une entreprise de commerce électronique adresse sur le téléphone portable de l'un de ses clients une offre pour un téléviseur. Cette offre indique que les informations détaillées concernant l'entreprise, le téléviseur et les conditions de vente sont disponibles sur le site Internet de l'entreprise, dont elle donne l'URL. Le client commande l'article sans consulter la page Internet. Lorsqu'il reçoit la facture, celui-ci est surpris par l'importance des frais de manutention et d'expédition. Il se plaint auprès de l'entreprise, mais celle-ci l'informe que tous les détails concernant les coûts étaient consultables sur le site Internet.

Dans l'exemple ci-dessus, l'entreprise de commerce mobile semble respecter les obligations d'information contenues dans la Section III de la Partie II, des *Lignes directrices sur le commerce électronique*. On peut toutefois se demander si l'information, qui ne serait disponible que sur Internet, serait aisément accessible aux utilisateurs d'un téléphone portable. Certains consommateurs peuvent ne pas avoir accès à Internet que ce soit par téléphone mobile ou depuis un ordinateur. Face à ce problème, les gouvernements pourraient, en faisant valoir d'autres dispositions des *Lignes directrices sur le commerce électronique* comme celles de la Partie III (« Mise en œuvre »), encourager les commerçants mobiles à :

- Fournir par SMS des informations précontractuelles de base, tout en reconnaissant que ce n'est qu'une solution partielle du fait des limitations actuelles que les opérateurs de communication ont imposées sur la longueur de ces messages et sur l'impossibilité d'imprimer ce type d'information.
- Envoyer par courrier imprimé les informations complètes à l'abonné mobile ayant exprimé son intérêt pour l'offre commerciale.
- Proposer un numéro téléphonique que les consommateurs peuvent appeler pour obtenir davantage de détails concernant leurs achats.
- De plus, les gouvernements pourraient, pour remédier à ces problèmes :
- Promouvoir des mécanismes et pratiques exemplaires d'autorégulation et encourager le secteur privé à prendre l'initiative dans le développement de la technologie, de telle manière que les consommateurs puissent aisément accéder à l'information complète dont ils ont besoin pour décider d'effectuer ou non une transaction.

Dans l'avenir, les nouvelles technologies permettant des communications sans fil de données sur de longues distances pourraient être intéressantes, dans la mesure où elles faciliteraient les transferts de données entre équipements mobiles et ordinateurs.

Processus de confirmation

Abonnement non souhaité

Un consommateur consulte avec son téléphone portable un site Internet proposant un accès en ligne gratuit d'un mois à une revue professionnelle. Il donne ses coordonnées par SMS pour accepter l'offre. Il n'a toutefois pas remarqué qu'il était indiqué dans les conditions contractuelles en bas de la page qu'au bout d'un mois le service deviendrait payant ; pour pouvoir lire ces informations, il lui aurait fallu faire défiler de nombreux écrans. Le consommateur est surpris quand au bout de deux mois il reçoit par SMS sa facture de téléphonie mobile sur laquelle est facturé le service en question ; il ne se rappelle pas avoir indiqué qu'il souhaitait s'abonner à la fin de la période d'essai.

Dans l'exemple ci-dessus, le consommateur a accédé à un site mais n'a pas confirmé son intention de souscrire au service à la fin de la période d'essai. Le prestataire de service a néanmoins prétendu que le consommateur avait bien passé commande.

Le scénario ci-dessus donne à penser que les utilisateurs de téléphonie mobile devraient avoir la faculté de recevoir des informations claires et complètes sur la transaction proposée afin de pouvoir, avant la conclusion du contrat, confirmer la commande des biens ou services en question, corriger toute erreur et, par ailleurs, conserver ou imprimer des traces adéquates de la transaction proposée effectuée au moyen d'un terminal mobile, notamment les conditions contractuelles (*Lignes directrices sur le commerce électronique*, Partie II, Section II et IV). Dans le cas où un abonné de téléphonie mobile ne reçoit pas une telle information préalable, il pourrait être judicieux de :

- Donner aux abonnés mobiles la faculté, dans les transactions mobiles, de suspendre le processus de transaction jusqu'à ce qu'ils aient eu la possibilité d'examiner l'intégralité du contrat et d'exprimer un consentement informé et délibéré à l'achat.

De plus, les abonnés de téléphonie mobile devraient être protégés contre les entreprises de commerce mobile déloyales ou peu scrupuleuses à même, grâce à l'information qu'elles obtiennent sur l'identité de ceux qui consultent leurs sites, d'exploiter ou de harceler ces personnes. Pour protéger les abonnées de téléphonie mobile contre ces risques, on pourrait, notamment dans les juridictions où la protection en vigueur n'est pas adéquate, mettre en place des règles limitant les informations (autres que les informations d'annuaire telles que nom et numéro de téléphone) que les opérateurs de téléphonie mobile peuvent communiquer à des tiers, sans le consentement du client, notamment à des partenaires dans le cadre de co-entreprises ou à des sous-traitants indépendants à des fins de marketing. D'autres mécanismes sont également envisageables, comme des règles imposant aux opérateurs mobiles de préciser de façon bien visible quelles sont leurs règles en matière de collecte de données.

Achat de titres

Un consommateur se connecte avec sa banque pour passer un ordre de vente d'actions sur son téléphone portable. Il valide les détails de l'ordre, pensant qu'il a confirmé la transaction. Or il ne voit pas qu'il lui faut aller jusqu'en bas de la page de validation pour accéder à l'information sur le processus de confirmation. La procédure de confirmation de l'ordre n'étant pas clairement expliquée, l'ordre n'est pas exécuté.

Dans l'exemple ci-dessus, le prestataire de services financiers a signalé au consommateur qu'il devrait effectuer la vente, mais néanmoins il ne lui a pas donné la possibilité d'en apporter la confirmation. Il convient de s'assurer que les procédures pour la réalisation de transactions sur les téléphones portables prennent en compte les limitations concernant par exemple la taille de l'écran et la capacité de stockage. Une fois que l'information de base concernant un ordre a été fournie, il serait intéressant pour les consommateurs :

- Qu'ils reçoivent confirmation de la transaction par un SMS ou un courrier électronique.
- Qu'ils aient la possibilité de vérifier aisément l'état d'exécution de leur ordre, sur leur combiné portable comme sur Internet.

Règlement des litiges et réparation

La Section VI de la Partie II des *Lignes directrices sur le commerce électronique* (« Règlement des litiges et recours ») encourage les entreprises à mettre en place des voies de règlement des litiges et de recours justes et rapides, transparentes et internes, pour le traitement des plaintes. Ces principes sont explicités plus en détail dans la *Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation* qui invite les participants du secteur privé à mettre en place « des procédures efficaces de traitement des recours internes offrant aux consommateurs la possibilité de régler leurs litiges directement avec l'entreprise concernée d'une manière équitable, efficace et rapide, sans imposer de frais ou charges pour pouvoir accéder à ou utiliser ces procédures ».

Imbrication de contrats

Télévision interactive

Une émission de recherche de talents à la télévision invite les téléspectateurs à voter pour leur candidat favori par SMS sur leur téléphone portable. Le prix de l'appel n'apparaît dans le bas de l'écran en tout petits caractères que pendant 10 secondes. De plus, les caractères sont impossibles à lire à la distance à laquelle se place normalement un téléspectateur par rapport à son téléviseur. Il n'y a pas de procédure de confirmation sur le téléphone portable – après avoir voté, le téléspectateur voit simplement s'afficher un message le remerciant de son vote. Les utilisateurs de téléphone portable ne peuvent savoir qu'on leur facture un service surtaxé que lorsqu'ils consultent leur facture de téléphone portable. Ceux qui contestent cette facturation auprès de leur opérateur de téléphonie mobile sont informés qu'ils sont tenus d'acquitter la facture et qu'il leur appartient de se retourner vers la société de télévision.

Titre de transport mobile

Un consommateur achète un titre de transport auprès d'une compagnie nationale de chemin de fer via son téléphone portable, lui permettant, grâce au protocole de communication dont est équipé son téléphone, d'utiliser celui-ci comme un titre de transport dans les autobus, trains et tramways. Alors qu'il circule à bord d'un tramway, il est contrôlé par un receveur qui tente de vérifier la validité du ticket mobile, mais sans succès. Le contrôleur demande donc au consommateur d'acquitter immédiatement le prix du ticket ainsi qu'une amende, le consommateur étant dans l'impossibilité de prouver qu'il a bien acheté le titre de transport. De retour chez lui, le consommateur demande à son opérateur mobile de l'aider à obtenir le remboursement du prix du billet et de l'amende.

L'opérateur mobile dégage sa responsabilité dans cette affaire et informe le consommateur qu'il doit adresser sa demande à la compagnie de chemin de fer.

Le premier exemple met en évidence l'interaction entre deux médias – la télévision traditionnelle et le commerce par terminal mobile. Il attire l'attention sur la tendance à l'utilisation des services de messages surtaxés comme modèle économique du commerce mobile. Cet exemple hypothétique soulève également un certain nombre de questions pour les abonnés à la téléphonie mobile notamment : *i*) l'impossibilité pour les consommateurs de savoir s'ils accèdent à des services surtaxés sur leur portable, *ii*) l'absence d'un processus de confirmation, et *iii*) l'absence chez l'opérateur de téléphonie mobile d'un système de règlement des litiges et de réparation en cas de contestation de facture.

En ce qui concerne le règlement des litiges, dans les deux exemples on voit qu'il existe un manque de clarté quant à savoir quelle est l'entité directement responsable du traitement des réclamations des consommateurs. Le plus souvent, les transactions de commerce mobile sont imputées sur la facture de téléphonie mobile de l'abonné pour le compte du vendeur des biens ou services commercialisés sur plateforme mobile. Il se peut même que les relations dans la prestation de services de commerce mobile soient encore plus complexes, notamment quand le paiement du service offert est débité sur le compte bancaire ou le compte de la carte de crédit du consommateur, comme le montre le deuxième exemple ci-dessus.

Dans quelques pays de l'OCDE, des partenariats ont été mis en place ou sont en voie de l'être entre entreprises de transport et opérateurs de téléphonie mobile pour offrir aux consommateurs la capacité d'utiliser leur téléphone portable comme titre de transport. Dans ces pays, les consommateurs sont débités selon différentes méthodes : sur leurs factures de téléphonie mobile, leurs cartes de crédit, ou bien en espèces. Dans ces transactions multipartites, le consommateur doit savoir clairement quelle est l'entité responsable du traitement des litiges de consommation et de la fourniture de voies de recours.

On voit avec les deux exemples ci-dessus qu'il serait intéressant d'encourager les opérateurs de téléphonie mobile et les commerçants à :

- Mettre en place des mécanismes internes équitables, efficaces et transparents pour l'enregistrement des plaintes des consommateurs et leur traitement.
- Indiquer clairement aux consommateurs les règles de responsabilité pour le traitement des litiges dans les contrats complexes. Des pratiques exemplaires pourraient à cet égard donner des indications sur l'identité de celui qui, opérateur de téléphonie mobile, entreprise de transport ou les deux solidairement, devrai(en)t être tenu(s) responsable(s) vis-à-vis des consommateurs en fonction des circonstances et caractéristiques particulières du litige.

De plus, les acteurs du commerce mobile devraient envisager la mise en place de mécanismes de règlement des litiges et de réparation tels que des codes de satisfaction client, des mécanismes de remboursement et des services alternatifs de règlement des litiges, comme indiqué dans la *Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation (Recommandation sur le règlement des litiges de consommation et leur réparation*, Annexe, Section II, A.7).

Il serait intéressant que les opérateurs de téléphonie mobile, les entreprises de commerce mobile, les opérateurs de sites Internet, les agrégateurs mobiles et les pouvoirs publics œuvrent ensemble pour la mise en place de mécanismes, politiques et procédures d'autorégulation équitables, efficaces et transparents pour le traitement des plaintes de consommateurs et le règlement des litiges de consommation découlant de transactions complexes de commerce mobile.

Litiges transfrontières

Montre de luxe

Un consommateur reçoit un SMS contenant un lien vers un site Internet faisant la publicité d'une montre de luxe à très bas prix. Le consommateur n'a pas de raison de douter que l'offre est réelle car elle émane d'un site mobile auprès duquel il a déjà acheté des produits similaires et elle contient des informations dans sa langue natale. Il commande donc la montre. Celle-ci tardant à être livrée, le consommateur se plaint auprès du service consommateur de l'entreprise et découvre que l'entreprise auprès de laquelle il a acheté l'article était de fait gérée par une autre société, non basée dans son pays. Lorsqu'il se plaint auprès de ses autorités, on lui dit qu'on ne peut rien faire dans la mesure où la société est implantée à l'étranger.

Dans la Partie II, Section III, A *i*) et *iii*) des *Lignes directrices sur le commerce électronique* les entreprises sont invitées à fournir aux consommateurs des informations les concernant de manière exacte, claire et facilement accessible, y compris les informations concernant leur localisation géographique et les mécanismes de résolution des litiges. Ces mécanismes d'information et de recours sont nécessaires pour renforcer la confiance des consommateurs dans les transactions transfrontières, comme l'indique également la *Recommandation de l'OCDE sur le règlement des litiges de consommation et leur réparation* qui invite les pays membres à renforcer l'efficacité des voies de recours à la disposition des consommateurs dans les litiges transfrontières (Annexe, Section III).

Les parties prenantes sont encouragées à mettre en place des mécanismes de résolution des litiges efficaces, pour traiter les plaintes des consommateurs dans les transactions transfrontières de commerce mobile.

Accès des consommateurs désavantagés au commerce mobile

Comme indiqué dans la *Recommandation de l'OCDE sur le règlement des litiges de consommation et leur réparation* (Annexe, Section II, A. 6), les besoins particuliers des consommateurs désavantagés devraient être pris en compte avec le développement du commerce mobile. Ainsi, il peut être particulièrement difficile pour des personnes malvoyantes de lire les notices d'information et d'exonération de responsabilité sur les petits écrans de terminaux mobiles.

III. Protection des mineurs

Dans la plupart des pays membres de l'OCDE, les mineurs (à savoir en général les personnes de moins de 18 ans) n'ont pas la capacité juridique de conclure des contrats commerciaux – tels que les abonnements de téléphonie ou les transactions commerciales sur téléphone portable. Cela toutefois ne les empêche pas de réaliser des transactions commerciales au moyen d'un équipement faisant l'objet d'un contrat souscrit par leurs parents ou un autre adulte. Dans certains pays, les mineurs d'un certain âge peuvent toutefois être autorisés à conclure de tels contrats, sous réserve d'un accord parental. Ce contrôle parental sur les activités commerciales des mineurs est actuellement remis en cause sur le marché du commerce mobile par l'augmentation rapide du nombre de mineurs disposant de leur propre terminal (OCDE 2006, p. 5-6). Un moyen de décourager les mineurs de conclure indûment des contrats pourrait être le suivant :

- Encourager les opérateurs mobiles à mettre en place des systèmes de vérification de l'âge.

Jusqu'à présent toutefois, les technologies de vérification de l'âge ne se sont guère diffusées, ce qui constitue un problème. Les opérateurs mobiles peuvent s'efforcer d'obtenir des informations sur l'âge d'une manière qui décourage toute falsification, par exemple en demandant aux enfants d'indiquer leur date de naissance, plutôt que simplement leur âge ; toutefois, en l'absence de technologie de vérification de l'âge, il n'est pas difficile pour des enfants de se soustraire aux mécanismes de contrôle de l'âge d'un site en donnant de fausses informations pour avoir ainsi accès à des sites qui ne leur sont pas destinés ou s'engager dans des transactions sans l'autorisation de leurs parents. Cela démontre le besoin de

technologies additionnelles permettant de renforcer la sécurité des enfants, dans la mesure où ceux-ci sont de plus en plus nombreux à s'engager dans des activités en ligne depuis des terminaux sans fil.

Les parents donnent en général à leurs enfants des téléphones portables pour mieux rester en contact avec eux et renforcer leur sécurité, mais l'usage qu'en font les enfants va bien au-delà (OCDE, 2006, p. 8). Ceux-ci sont de plus en plus attirés par des services qui peuvent se révéler payants (comme le téléchargement de sonneries, de vidéos, de « chats » et de jeux). Dès lors, ceux-ci s'engagent dans des transactions commerciales et peuvent être exposés à des risques tels que *i*) l'accès à des contenus préjudiciables réservés aux adultes et *ii*) des transactions particulièrement coûteuses, pouvant résulter d'un marketing agressif.

La Section II de la Partie II des *Lignes directrices sur le commerce électronique* stipule que « les entreprises devraient prendre un soin tout particulier dans la publicité ou le marketing destinés aux enfants, qui peuvent ne pas être en mesure de comprendre pleinement les informations qui leur sont présentées ». Ce principe devrait guider les fournisseurs de services mobiles, les opérateurs de téléphonie mobile et les autres entités offrant des services de commerce mobile dans les communications et transactions avec des enfants.

Accès à des contenus préjudiciables ou pour adultes

Réservé aux adultes

Un adolescent de 15 ans reçoit un message l'invitant à consulter gratuitement en avant-première un nouveau site sur Internet. L'adolescent répond au message en demandant l'adresse du site, auquel il se connecte et découvre alors que celui-ci propose des contenus sexuellement explicites. Il en parle à sa mère, qui contacte immédiatement l'opérateur de téléphonie mobile pour dire qu'elle est choquée que son fils ait été ainsi sollicité. L'opérateur mobile explique qu'il fait de son mieux pour filtrer ce type de trafic, mais que certains messages inappropriés échappent au filtre. Quand l'adolescent a répondu au SMS, ses coordonnées (c'est-à-dire son numéro de portable) ont été ajoutées à une liste de clients potentiels. Il a par la suite reçu toute une série de messages provocants, contraignant la mère désemparée à demander l'ouverture d'un nouveau compte de téléphonie mobile pour son fils.

Site de photos gratuites

Un adolescent de 15 ans apprend par des amis l'existence d'un site de photos gratuites pour adultes. Il se connecte sur ce site au moyen de son téléphone portable, sachant que ses parents ne pourront pas suivre ses activités sur l'Internet de près. Le site Internet comporte un avertissement stipulant que l'accès est réservé aux personnes de plus de 18 ans. L'adolescent répond qu'il remplit cette condition et obtient immédiatement l'accès au site.

Les entreprises devraient étudier l'élaboration d'outils plus efficaces pour empêcher les mineurs d'accéder depuis leur portable à des sites présentant des contenus pour adultes. Comme indiqué dans les *Lignes directrices sur le commerce électronique*, les pays membres « devraient… encourager le secteur privé à continuer d'assumer un rôle pilote dans le développement technologique en tant que moyen de protéger les consommateurs et de leur donner plus de pouvoir » (Part III, iii), « Mise en œuvre »).

Beaucoup a été fait pour développer des logiciels conçus justement pour filtrer certains contenus et éviter qu'ils ne parviennent jusqu'aux consommateurs qui utilisent leur ordinateur pour accéder à l'Internet. Face à ce problème dans l'environnement du commerce mobile, des codes de conduite volontaires ou des lignes directrices ont été élaborés par les opérateurs mobiles dans certains pays en vue de mettre en place des options restreignant l'accès des enfants aux contenus pour adultes (Appendice I.1). Dans ces systèmes, les opérateurs mobiles ont soutenu un certain nombre d'actions destinées à répondre aux problèmes associés aux mineurs, notamment :

- Le développement de campagnes de sensibilisation des parents et des enfants.
- Mettre en garde dans toutes les publicités sonores et visuelles que les parties intéressées doivent être âgées de 18 ans ou plus ou avoir l'autorisation des parents pour participer.
- Classifier les contenus commerciaux (contenus réservés aux adultes d'une part et contenus généralement accessibles d'autre part).
- Élaborer des procédures plus efficaces de vérification de l'âge.

Un certain nombre d'autres mesures pourraient être explorées pour protéger les mineurs :

- Adapter à l'environnement mobile les lois et règles en vigueur dans les pays membres pour protéger les enfants en ligne.
- Encourager les opérateurs mobiles à informer les parents des options de filtrage à leur disposition pour les aider à empêcher leurs enfants d'accéder aux contenus pour adultes.
- Encourager les commerçants mobiles vendant des services de contenus pour adultes *i*) à travailler avec les autorités compétentes au niveau national pour assurer une protection efficace des mineurs et *ii*) à mettre en place des mesures de protection appropriées pour empêcher l'accès des enfants à ces services.
- Établir des procédures par lesquelles, par exemple, les parents sont notifiés que leurs enfants accèdent à des sites pour adultes ; et
- Prévoir des services de filtrage pouvant être activés par les parents sur le terminal pour bloquer l'accès via Internet à des contenus inappropriés.

Marketing en direction des enfants

Sonneries et autres produits

Une adolescente de 13 ans est intriguée par divers messages qu'elle reçoit sur son téléphone portable émanant d'un commerçant auprès duquel elle a auparavant acheté une sonnerie. Le commerçant l'encourage à acheter toutes sortes de produits et de services. Elle finit par acheter un certain nombre d'autres sonneries, jeux et horoscopes. Sa mère demande à l'opérateur mobile d'intercepter les publicités, mais celui-ci indique qu'il est dans l'incapacité de le faire.

Publicités non sollicitées

Un enfant de dix ans fait des courses dans un centre commercial avec sa maman. En passant devant des boutiques, il est intrigué par les publicités qui lui sont adressées sur son téléphone mobile par divers commerçants. Il le montre à sa mère, qui est impressionnée par cette nouvelle fonction de son téléphone. Elle ne connaissait pas les propriétés de la technologie Bluetooth dont est équipé le téléphone de son fils. De retour chez elle, la mère s'inquiète des aspects négatifs que pourrait avoir cette publicité non sollicitée rendue possible par la technologie Bluetooth.

Comme indiqué dans les *Lignes directrices sur le commerce électronique* (Section II de la Partie II), les enfants peuvent ne pas avoir la capacité de comprendre pleinement l'information qui leur est présentée. S'il peut être difficile de prévenir le marketing mobile abusif ciblant les enfants, il peut exister des moyens de le limiter en encourageant les opérateurs mobiles à mettre en place des outils qui permettraient :

- D'éduquer les parents en même temps que les enfants sur les techniques de marketing agressives et les moyens de limiter les dépenses via les terminaux mobiles.
- D'empêcher certains publicitaires, ou types de publicitaires, d'envoyer des publicités aux enfants.
- De placer des restrictions sur l'accès aux contenus sur Internet.
- De bloquer les achats par téléphone portable sur les équipements confiés aux enfants mineurs.
- De bloquer tous les messages mobiles autres que ceux émanant de sources identifiées par les parents (liste blanche).

Les commerçants mobiles pourraient également être encouragés à exiger l'autorisation d'adultes pour toutes les transactions de commerce mobile émanant de parties qu'ils savent être des mineurs.

L'exemple relatif à la *Publicité Non Sollicitée* soulève un autre type de problème. Dans ce cas de figure, les publicités sont diffusées directement par *Bluetooth* pour être captées sur le téléphone de l'enfant. Cette forme de publicité ne passe pas par les opérateurs mobiles et il n'en est gardé aucune trace. L'exemple montre que les parents doivent être conscients des capacités techniques et fonctions des téléphones portables donnés à leurs enfants. Ils doivent savoir comment configurer ces fonctions quand des problèmes se posent.

Surconsommation de services offerts par les opérateurs mobiles

Distributeur de boissons sans alcool

Une adolescente de 12 ans est enchantée d'être élue déléguée de sa classe. A la pause déjeuner, elle décide d'offrir une tournée de boissons sans alcool à ses camarades de classe. La nouvelle se répand rapidement et bientôt 300 jeunes se présentent. Elle utilise son téléphone portable pour payer les boissons. Le montant total apparaît sur l'écran de son téléphone. Quand il reçoit la facture mensuelle, son père est abasourdi de voir que celle-ci s'élève à EUR 400.

Jeux interactifs

Un adolescent de 16 ans reçoit un téléphone portable pour son anniversaire. Sa mère le met en garde contre les risques de factures élevées. Le jeune homme acquiesce, et s'efforce de tenir parole. Toutefois, voyant que les messages textuels et jeux interactifs sont très bon marché, il utilise beaucoup ces services sans se rendre compte que l'accumulation d'un grand nombre de petits montants conduit à une somme rondelette. La facture mensuelle totale dépasse USD 200.

Comme illustré dans les exemples ci-dessus, les parents ne sont pas toujours en mesure de superviser en permanence les activités de leurs enfants sur leur téléphone portable. De ce fait, ils peuvent être dans l'impossibilité de les empêcher d'accumuler des sommes significatives sur leurs factures téléphoniques pour des services ou produits qu'ils achètent. Les jeux et concours à la télévision sont des activités dans le cadre desquels les mineurs semblent particulièrement vulnérables. Comme illustré plus haut dans l'exemple relatif à la *Télévision Interactive*, l'information sur les coûts de la participation à ces jeux n'est pas toujours clairement disponible.

Les distributeurs de boissons dans les écoles ou les centres commerciaux sont un autre exemple de tentation pour les mineurs. Avec leur téléphone portable, les mineurs peuvent parfois appeler un numéro de téléphone affiché sur la machine et acquitter ainsi leur achat, qui sera débité sur leur prochaine facture téléphonique.

Les services surtaxés, comme on l'a vu précédemment, peuvent aussi être une tentation pour les jeunes consommateurs. Il s'agit de services offrant des informations et des distractions sur divers supports, notamment téléphone fixe, télécopie, Internet, télévision et terminaux portables. Les enfants peuvent ainsi facilement effectuer un appel depuis leur téléphone portable pour accéder à un large éventail de services qu'il s'agisse de concours, de dialogues en direct, *etc.* En général, les appels vers ces services sont facturés plus chers que les appels standard. Les professionnels peuvent apporter une aide en continuant d'élaborer et d'améliorer des outils technologiques permettant de limiter la consommation de services mobiles par les mineurs. De tels outils iraient dans le sens des *Lignes directrices sur le commerce électronique* (Partie II, Section III, C. *v*) qui invitent les entreprises à donner aux consommateurs des informations sur les restrictions, limitations ou conditions d'achat, telles que l'accord des parents ou du tuteur, ou les restrictions de lieux ou de temps.

L'approche utilisée par les sociétés de carte de crédit peut être utile à cet égard. Lorsqu'une carte a été délivrée à une personne, les entreprises permettent souvent, avec l'accord du titulaire, la délivrance de cartes additionnelles aux autres membres

de la famille, dans les limites de crédit fixées par le souscripteur principal. Les lignes de crédit peuvent être limitées, et les factures sont adressées pour paiement au souscripteur principal. De plus, dans certains pays, les mineurs ne peuvent détenir de cartes de crédit, à moins que les parents ne l'autorisent expressément dans le contrat.

Quelques pays sont allés plus loin (Appendice I.1), en impliquant davantage les opérateurs mobiles. Dans un pays, pour les jeux télévisés auxquels on participe par SMS, les opérateurs mobiles doivent rembourser aux parents les factures encourues par leurs enfants. Dans un autre pays, les fournisseurs de contenus qui ne fixent pas une limite mensuelle aux achats de leurs services effectués depuis un numéro d'accès peuvent être considérés comme enfreignant la loi.

Pour réduire les risques de surconsommation, les parties prenantes pourraient :

- Donner aux parents la possibilité de plafonner le montant des factures que les enfants peuvent accumuler via leur téléphone portable, par exemple en restreignant le nombre de messages textuels ou en plafonnant le montant des achats par téléchargement.
- Encourager une conception des terminaux mobiles permettant aux utilisateurs d'interdire certains types de transaction.
- Encourager les opérateurs mobiles à adresser des mises en garde ou avis aux parents quand les dépenses dépassent un plafond prédéterminé.

Les enfants et les données de géolocalisation[1]

Pistage par téléphone

Une adolescente de 12 ans accède via son téléphone portable à l'Internet et donne son numéro de portable pour s'inscrire à un service de géolocalisation lui permettant de savoir où se trouvent les personnes qu'elle a indiquées (géolocalisation sociale). Elle pense qu'il sera ainsi amusant de voir si des amis de classe sont à proximité, et de leur adresser un SMS pour les rencontrer. Ceux-ci peuvent de leur côté recevoir des informations sur sa propre localisation et son profil. Aucune indication n'est donnée par le service sur la façon dont ces données seront protégées, ou sur l'identité de ceux qui peuvent les consulter. Il n'y a aucune procédure de validation. Les données de localisation ne sont pas bloquées même quand l'intéressée désactive le programme sur son téléphone portable. Ses parents ignorent qu'elle s'est inscrite à un tel service.

L'exemple ci-dessus illustre les problèmes soulevés à l'intersection de la vie privée, de l'activité en ligne et du commerce mobile s'agissant des enfants. D'autres questions en relation avec la vie privée, qui peuvent affecter aussi bien les enfants que les adultes, sont examinées plus loin dans la section sur les questions de vie privée et de sécurité en relation avec la géolocalisation. Dans de nombreux pays de l'OCDE, il est illégal de communiquer à des tiers des informations de géolocalisation ; toutefois un certain nombre de questions restent en suspens concernant

1. Les données de géolocalisation sont des données indiquant la position géographique et les déplacements d'un équipement mobile.

l'étendue de cette protection dans certains pays. Le problème du manque d'informations sur les données de localisation et de l'échange d'information avec des tiers est amplifié dans beaucoup de pays par l'absence d'un processus permettant d'alerter les adultes sur ces pratiques. Alors qu'une information plus complète pourrait aider à faire face au problème, cela ne serait cependant pas suffisant.

Les *Lignes directrices sur le commerce électronique* définissent déjà plusieurs principes généraux qui pourraient s'appliquer, notamment le principe selon lequel les entreprises faisant commerce avec des consommateurs ne devraient pas s'engager dans des pratiques susceptibles de présenter pour ceux-ci des risques de préjudices déraisonnables (Section II, Partie II, 2ème paragraphe) ; et que les entreprises devraient présenter des informations les concernant et décrivant les biens ou services qu'elles offrent d'une façon claire, visible, exacte et facilement accessible (Section II, Partie II, 3ème paragraphe). En l'occurrence, l'information de localisation pourrait être considérée comme relevant du principe selon lequel l'entreprise doit fournir une information suffisante sur les termes, conditions et coûts associées à une transaction pour permettre aux consommateurs de décider de façon éclairée s'ils souhaitent ou non conclure la transaction. Cette information doit être claire, exacte et facilement accessible. Comme mentionné plus haut, les *Lignes directrices sur le commerce électronique* encouragent également le secteur privé à prendre l'initiative dans le développement de la technologie en tant qu'outil destiné à protéger et autonomiser les consommateurs (Partie III, *iii*)). A cette fin, les entreprises pourraient :

- Donner une information claire sur la géolocalisation.
- Donner une information claire sur l'échange de données avec des tiers et la façon de limiter cet échange.
- Traiter ce service comme nécessitant l'accord d'un adulte.
- Offrir la possibilité de désactiver le service spécifique de géolocalisation, de préférence par défaut.

IV. Utilisation frauduleuse de terminaux mobiles et questions de sécurité

La petite taille et les fonctionnalités des terminaux mobiles en font des cibles attrayantes pour les voleurs, qui peuvent être intéressés par *i*) l'utilisation ou la revente de l'équipement, *ii*) la réalisation de transactions commerciales de façon frauduleuse ou illégale au nom du propriétaire légitime ou *iii*) l'obtention de données personnelles sensibles. Le risque de vol est à bien des égards beaucoup plus élevé que pour les ordinateurs standard, qui sont fixes, ou les ordinateurs portables, beaucoup plus encombrants, que l'on emporte moins souvent avec soi dans les lieux publics.

Utilisation frauduleuse de téléphones portables

Le fait de mieux sensibiliser aux risques de l'utilisation non autorisée des téléphones portables devrait contribuer à réduire le nombre d'incidents. Comme indiqué dans la Section VIII de la Partie II des *Lignes directrices sur le commerce électronique,* les parties prenantes « … devraient collaborer en vue d'assurer l'éducation des consommateurs en matière de commerce électronique … et de

sensibiliser davantage les entreprises et les consommateurs aux cadres de protection des consommateurs qui s'appliquent à leurs activités en ligne. » L'information des consommateurs sur ce qu'ils devraient faire en cas de vol ou de piratage de leur terminal mobile est un autre aspect important de la prévention des usages frauduleux. Les acteurs devraient dont œuvrer ensemble :

- Pour fournir des informations aux consommateurs qui *i*) contribuent à leur sensibilisation, *ii*) suggèrent des moyens de protéger les terminaux mobiles contre les risques de perte ou d'usage frauduleux et *iii*) indiquent ce que les consommateurs devraient faire s'ils constatent que leur terminal a été volé ou a été utilisé de façon frauduleuse.

Accumulation de factures

Un consommateur perd son téléphone portable sans toutefois en informer ni son opérateur mobile ni la police, car il pense qu'il va le retrouver rapidement. Trois jours plus tard, la police l'appelle pour lui signaler que son téléphone a été retrouvé. Toutefois, entre le moment où le téléphone a été perdu et celui où la police l'a retrouvé, quelqu'un a utilisé ce téléphone pour acheter des services mobiles coûteux, pour un montant d'environ USD 2 000. Le consommateur est choqué d'apprendre que la totalité du montant lui est imputable.

L'exemple ci-dessus montre l'importance d'utiliser les sécurités offertes par une forme ou une autre de chiffrement sur le terminal lui-même, de même qu'un numéro d'identification personnel pour certains services. Il montre aussi l'importance de signaler rapidement la perte d'un terminal mobile. D'autres possibilités existent pour limiter la responsabilité en cas de vol :

- Permettre aux consommateurs de fixer des plafonds de crédit qui peuvent être inférieurs à ceux à partir desquels s'applique la responsabilité limitée définie par les opérateurs de téléphonie mobile.
- Proposer des services à distance et autres dispositifs techniques sur demande permettant aux consommateurs de bloquer leur terminal pour empêcher son utilisation non autorisée.
- Imposer l'utilisation d'un code PIN pour chaque transaction commerciale effectuée sur le terminal mobile, ou pour accéder à des informations sensibles sur l'appareil.
- Éduquer les consommateurs sur l'importance d'utiliser des mots de passe et autres dispositifs limitant l'accès à ce type d'équipements.

En ce qui concerne le code PIN de la carte SIM, le code initial par défaut est généralement « 0000 »[2].

- Pour dissuader les utilisations non autorisées, les opérateurs de téléphonie mobile et les vendeurs de téléphones pourraient *i*) attribuer des codes PIN initiaux aléatoires et/ou *ii*) inciter les consommateurs à changer le code PIN

2. Cette observation n'est pas valable pour les réseaux de téléphonie mobile utilisant la technologie CDMA (Code Division Multiple Access) dans certains pays de l'OCDE.

par défaut et à saisir un code personnel lorsqu'ils utilisent pour la première fois le terminal.

Ligne occupée

Une jeune femme perd son téléphone portable dans l'autobus en rentrant chez elle de son travail. Lorsqu'elle découvre le vol, elle appelle immédiatement son opérateur mobile. Elle doit renouveler l'appel plusieurs fois, car la ligne est occupée. Lors de l'un de ces appels, elle finit par raccrocher, après avoir attendu 20 minutes un conseiller clientèle. Elle est furieuse plusieurs jours plus tard d'apprendre que son téléphone a été utilisé pour acheter pour EUR 1 000 de services pendant la période où elle a essayé sans succès de contacter l'opérateur mobile.

Le fait de tenir les abonnés mobiles responsables des factures non autorisées effectuées aux moyens de terminaux mobiles volés pendant la période où ils n'ont pu notifier leur opérateur du vol car les lignes étaient occupées ou pour d'autres raisons de même nature, soulève des questions d'équité. Cette inaccessibilité pourrait exposer les abonnés à des risques de préjudices déraisonnables, ce qui est contraire aux dispositions des *Lignes directrices sur le commerce électronique*, et à la *Recommandation sur le règlement des litiges de consommation et leur réparation* (Partie IV) qui invite le secteur privé à proposer aux consommateurs des mécanismes pour résoudre leurs différends le plus rapidement possible. Pour éviter de telles situations, les opérateurs mobiles pourraient être encouragés à :

- Offrir aux abonnés des moyens suffisants pour signaler rapidement leurs ennuis, notamment un service de courrier électronique ou « en ligne » pour déclarer les terminaux perdus ou volés.
- Mettre en place des lignes d'appel spéciales pour les terminaux perdus ou volés, sur lesquelles les consommateurs pourraient taper au clavier l'information nécessaire pour désactiver l'appareil.

Des efforts pour améliorer les mécanismes de signalement des combinés perdus ont été faits dans un certain nombre de pays. Dans l'un d'entre eux, les opérateurs mobiles se sont regroupés et ont signé une charte pour bloquer les terminaux portables signalés volés sur l'ensemble de leurs réseaux dans un délai de 48 heures. Comme les terminaux portables comportent un numéro d'identification d'équipement mobile international (code IMEI)[3] qui est enregistré, chaque opérateur peut à distance verrouiller la carte SIM et le code IMEI pour bloquer l'appareil et le rendre inutilisable.

Il faut noter que lorsqu'un téléphone portable est utilisé comme moyen de paiement, la responsabilité n'est pas la même que pour une carte de crédit. Dans certains pays de l'OCDE, les consommateurs sont très souvent non responsables des montants débités au moyen d'une carte de crédit volée. Avec les téléphones portables utilisés comme terminal de paiement, les abonnés mobiles ne bénéficient pas d'un même niveau de protection. Les opérateurs mobiles dans la plupart des

3. Il est attribué aux équipements portables utilisant la technologie CDMA un numéro de série électronique (ESN ou Electronic Serial Number) destiné comme le code IMEI à identifier de façon unique chaque terminal.

pays membres ne couvrent pas les pertes qu'elles soient causées par l'utilisation non autorisée de cartes SIM ou de puces informatiques. Quelques pays toutefois ont modifié leur législation afin de limiter la responsabilité découlant de toutes les formes d'utilisation non autorisée de services de communication. Pour remédier à ce problème, les gouvernements et les professionnels pourraient envisager de :

- Voir s'il y aurait des moyens d'améliorer la protection en matière de responsabilité civile des utilisateurs de téléphones portables ; comme l'indique les *Lignes directrices sur le commerce électronique* et la *Recommandation sur le règlement des litiges de consommation et leur réparation*, la limitation de la responsabilité du consommateur et les mécanismes de remboursement sont des outils puissants susceptibles d'aider à protéger les consommateurs.

Vacances à l'étranger

Une femme qui passe ses vacances d'été à l'étranger se fait voler son téléphone portable alors qu'elle fait ses courses sur un marché en plein air. Elle déplore cette perte mais ne craint pas outre mesure qu'il soit utilisé de façon abusive car son opérateur mobile lui a indiqué que son téléphone ne fonctionnerait pas à l'étranger car il n'est pas compatible avec le réseau de télécommunication. Elle ne signale donc pas la perte, jusqu'à ce qu'elle rentre chez elle. L'opérateur mobile lui apprend alors la mauvaise nouvelle. La facture sur son compte s'élève à quelque USD 20 000. S'il est certes exact que son téléphone ne fonctionne pas à l'étranger, l'opérateur mobile a oublié de lui indiquer que la puce (ou la carte SIM) peut être retirée du téléphone et utilisée dans un autre. L'entreprise reconnaît que la brochure d'information qu'elle lui a fournie n'est pas claire, mais insiste pour qu'elle paie. La plaignante porte l'affaire devant les tribunaux, qui lui donnent raison.

Dans l'exemple ci-dessus, l'opérateur mobile aurait du donner à sa cliente une information complète sur le fonctionnement de la puce de son téléphone à l'étranger. Comme indiqué dans la Section V de la Partie II des *Lignes directrices sur le commerce électronique*, les consommateurs devraient pouvoir disposer de mécanismes de paiement sûrs ainsi que d'informations sur le niveau de sécurité assuré par ces mécanismes. Ce principe revêt d'autant plus d'importance que le nombre de consommateurs utilisant leur téléphone portable à l'étranger augmente. Il faudrait donc s'attacher à :

- Faire en sorte que les abonnés mobiles bénéficient d'une information claire et complète sur la façon dont leurs terminaux mobiles peuvent être ou ne pas être utilisés à l'étranger au moment où ils achètent leur équipement ; et
- Mettre en garde les abonnés mobiles, lorsqu'ils achètent leur téléphone, que la puce du terminal peut être utilisée par une personne non autorisée, même si le terminal lui-même ne peut pas être utilisé à l'étranger.

Emprunt avec usurpation d'identité

Un collègue de bureau utilise le téléphone portable et le numéro d'appel d'un abonné pour souscrire un emprunt à l'insu de celui-ci. Pour valider cet emprunt, le collègue envoie un message donnant le nom de l'abonné. La société de prêt ne vérifie pas plus avant l'identité de l'expéditeur.

Le fait de permettre à des personnes d'utiliser leur téléphone portable pour effectuer des achats au nom d'autrui est contraire à la Section V des *Lignes*

directrices sur le commerce électronique sur deux points clés : *i*) la sécurité des paiements et *ii*) la loyauté des pratiques en matière de commerce, de publicité et de marketing (dans la mesure où cette pratique crée un risque déraisonnable de préjudice pour les consommateurs). Pour prévenir de telles pratiques, il pourrait être judicieux que les entreprises mettent en place des procédures et instruments de sécurité qui les aident à identifier la partie à un contrat conclu via un équipement mobile. Pour y remédier dans une certaine mesure, on pourrait prévoir de :

- Limiter l'ordre d'achat au seul titulaire du compte du terminal à partir duquel l'ordre est émis.
- Vérifier l'identité de l'abonné au moyen d'informations telles que l'envoi d'un SMS, une adresse de courrier électronique sur mobile, ou un code PIN.

Sécurité des mobiles

Piratage bancaire avec un téléphone portable

Un abonné à la téléphonie mobile reçoit une publicité pour des services bancaires mobiles gratuits où il est dit que l'application est accessible en tout lieu et à tout moment d'un simple clic. La publicité précise que les consommateurs peuvent consulter le solde de leur compte, faire des transferts entre comptes, et recevoir et acquitter des factures, comme ils le font d'ores et déjà avec leur ordinateur personnel. Il est précisé que pour protéger la vie privée et garantir la sécurité, toute les informations dans cette application de service bancaire mobile sont protégées par mot de passe et chiffrées, et il est prétendu en outre que le consommateur est ainsi protégé contre toute transaction non autorisée. La publicité contient un lien vers le formulaire d'enregistrement, qui est envoyé par SMS. L'abonné mobile complète le formulaire, accepte l'offre et commence à utiliser le service.

Le mois suivant, l'abonné mobile reçoit de son prestataire de services bancaires une facture contenant des montants importants correspondant à l'utilisation de l'application et à l'accès à ses données bancaires via son portable. La publicité de la banque ne mentionnait que cela était facturé. Le mois suivant, le consommateur apprend qu'un débit non autorisé a été effectué sur son compte bancaire. Il s'efforce de faire annuler la transaction par l'opérateur mobile mais celui-ci le renvoie vers sa banque, expliquant qu'après enquête, il apparaît que les données bancaires du consommateur n'étaient pas sécurisées et ont été piratées.

Ce cas hypothétique pose un certain nombre de problèmes pour les consommateurs concernant : *i*) la sécurité des combinés mobiles, notamment comme terminaux de paiement, *ii*) l'information sur le montant des frais d'accès aux données et *iii*) l'accès à des mécanismes appropriés de règlement des litiges et de réparation. La section ci-après met l'accent sur les questions de sécurité et de protection du consommateur dans les communications sans fil, comme pour les deux autres questions analysées plus haut en relation avec les exemples concernant la *Télévision Interactive, le Titre de Transport Mobile* et l'achat d'une *Montre de Luxe*.

Les terminaux mobiles s'apparentent de plus en plus à des mini-ordinateurs, capables d'effectuer un éventail croissant d'opérations, notamment de télébanque. La sécurité des réseaux sans fil qu'utilisent ces terminaux, qu'il s'agisse d'ordinateurs portables ou de terminaux plus petits, est de plus en plus souvent évoquée dans la presse. Un intrus peut pirater le terminal sans fil d'un consommateur ou le réseau, de la même manière que pour la plupart des ordinateurs disposant d'un accès Internet – par exemple au moyen d'un virus dans un courrier électronique. De plus, les pirates et autres intrus peuvent disposer de moyens

additionnels pour pirater les données contenues sur les terminaux mobiles [par exemple, liaison *Bluetooth*, puce RFID (Radio Frequency Identification)] ou infecter ces terminaux (par exemple, par le téléchargement d'applications). Bien que le spam et les logiciels malveillants soient actuellement moins répandus sur les terminaux mobiles que sur les ordinateurs, avec le développement de l'utilisation et de la valeur des transactions mobiles, on constate un intérêt croissant pour le piratage de données personnelles et financières et l'utilisation des terminaux mobiles pour des arnaques au spam, le vol d'identité, *etc*.

De plus, comme on l'a vu, l'utilisation des terminaux mobiles pour les paiements se généralise. Dans certains pays, les paiements mobiles sont généralement effectués par SMS, alors que dans d'autres, les terminaux sont équipés de puce RFID capables de transmettre les informations de paiement à des lecteurs par simple passage du terminal mobile devant un lecteur. Cela peut créer de nouveaux de risques pour la sécurité.

Les *Lignes directrices sur le commerce électronique* (Section II de la Partie II « Vie privée ») s'appliquent à cette situation dans la mesure où elles précisent que les activités de commerce électronique entre entreprises et consommateurs devraient être menées en conformité avec les principes reconnus pour la vie privée énoncés dans les *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980)* (« Lignes directrices sur la vie privée »), et des *Lignes directrices de l'OCDE de 2002 régissant la sécurité des systèmes et réseaux de l'information,* et en tenant compte de la *Déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux (1998)*. Il pourrait toutefois être nécessaire d'introduire des mesures additionnelles. Il pourrait être utile pour les participants au commerce mobile :

- De faire en sorte que les consommateurs soient informés des problèmes possibles d'atteinte à la sécurité et à la vie privée auxquels les expose le commerce mobile et des mesures à leur disposition pour limiter les risques.
- D'encourager l'élaboration de mesures de sécurité et de fonctions de sécurité intégrées.
- D'encourager les opérateurs mobiles à mettre en place des politiques et mesures de sécurisation des données destinées à prévenir les transactions non autorisées et les compromissions de données ; et
- De proposer aux consommateurs des moyens rapides et efficaces de recours quand leurs données sont compromises et/ou ils subissent un préjudice financier.

Questions de vie privée et de sécurité en relation avec la localisation

Localisation non autorisée

Un opérateur mobile utilise un système GPS (Global Positioning System) ou un système de triangulation (à partir des signaux émis par le terminal) pour localiser les utilisateurs mobiles. L'entreprise vend les informations concernant l'abonné et sa localisation à des entreprises de marketing qui les utilisent pour adresser à l'abonné mobile des publicités ou messages personnalisés. L'abonné mobile n'a pas compris que dans ce système ses données personnelles sont communiquées à autrui, et il n'a pas donné son accord à cet effet. Il peut arriver que des messages d'information lui soient facturés (par exemple facturation de SMS envoyés concernant les ventes proposées à proximité, ou du temps de connexion sur Internet pour l'affichage des messages « pop-up »). Il est troublé par le fait qu'on puisse savoir où il est, et inquiet que l'information puisse être interceptée (volée ou achetée) par des criminels.

L'exemple ci-dessus illustre les enjeux de l'information géolocalisée. Se pose le problème de l'absence de procédures pour protéger l'information et, comme dans le cas hypothétique examiné plus tôt en relation avec la protection des enfants (*Pistage*), de l'absence d'un mécanisme pour désactiver le positionnement pour des applications n'ayant pas un caractère d'urgence.

Le besoin de mesures de protection à l'égard des informations géolocalisées pourrait être couvert par le principe énoncé dans la Section VII de la Partie II des *Lignes directrices sur le commerce électronique* selon lequel les activités de commerce électronique entre entreprises et consommateurs devraient être menées en conformité avec les principes reconnus de protection de la vie privée énoncés dans les *Lignes directrices de l'OCDE de 1980 sur la vie privée* (Partie II, 7-10) et en tenant compte de la *Déclaration des ministres de l'OCDE de 1998 relative à la protection de la vie privée sur les réseaux mondiaux*.

Il serait judicieux que les entreprises :

- Donnent aux consommateurs des indications claires sur toutes les informations de localisation qui sont recueillies et sur l'usage auquel ces informations sont destinées.
- Donnent aux consommateurs la possibilité de restreindre l'échange de données avec des tiers (à l'exception des situations d'urgence), et de revenir sur leur décision concernant ceux avec lesquels ces données peuvent être échangées.

De plus, les entreprises qui recueillent des informations de positionnement devraient prendre des mesures appropriées pour protéger ces informations, notamment lorsqu'il s'agit de données sensibles ou qui peuvent être rattachées à une personne en particulier.

Appendice I.1
PROTECTION DES MINEURS : LÉGISLATIONS ET MÉCANISMES D'AUTORÉGULATION DANS CERTAINS PAYS DE L'OCDE

Accès aux contenus pour adultes

Des mesures ont été prises dans un certain nombre de pays pour faire face aux problèmes soulevés par les téléphones portables. En Allemagne, en Australie, en Corée, au Danemark, aux États-Unis, au Japon, en Norvège et au Royaume-Uni par exemple, les opérateurs mobiles ont élaboré des codes de conduite volontaires pour limiter l'accès aux contenus pour adultes. Aux États-Unis, certains opérateurs mobiles ont adopté des systèmes de classification volontaires des contenus et des contrôles d'accès à Internet afin de limiter l'accès aux contenus pour adultes et de permettre aux parents d'en garder la maîtrise (voir www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36). Ainsi, les opérateurs participants bloquent actuellement tous les sites Internet de contenus pour adultes, l'accès à ces contenus se faisant uniquement via un portail accessible aux seuls consommateurs âgés d'au moins 18 ans ou autorisés par un parent ou un tuteur. De plus, la Loi sur la protection des enfants sur Internet (Children's Internet Protection Act ou « CIPA ») impose aux écoles et bibliothèques participant au programme E-rate – lequel rend certaines technologies plus accessibles aux écoles et bibliothèques remplissant certains critères – de certifier qu'elles mettent en oeuvre une politique de sécurité sur Internet, comprenant des mesures techniques de protection destinées à bloquer ou filtrer l'accès par Internet aux contenus obscènes, contenant de la pédo-pornographie ou préjudiciables pour les mineurs.

Par ailleurs, l'Association pour le marketing mobile (MMA), qui est un groupe international promulguant des lignes directrices aussi bien en Europe qu'aux États-Unis, a récemment révisé ses lignes directrices sur les pratiques exemplaires aux États-Unis, concernant le marketing en direction des moins de 13 ans (voir www.mmaglobal.com/bestpractices.pdf). Ainsi, ces lignes directrices prévoient que pour avoir accès à des informations sonores et visuelles, les participants doivent être âgés d'au moins 18 ans ou avoir obtenu l'autorisation d'un parent. De même, en février 2007, d'importants opérateurs mobiles européens se sont mis d'accord sur un Cadre européen pour l'utilisation sans danger de mobiles par les adolescents et enfants (voir http://ec.europa.eu/information_society). Aux termes de ce Cadre, les opérateurs mobiles encouragent l'élaboration de campagnes de sensibilisation en direction des parents et des enfants, la classification des contenus commerciaux (séparation entre contenus réservés aux adultes et contenus accessibles par tous), et l'élaboration de procédures de vérification de l'âge.

Protection des données nominatives des enfants

Les pays pourraient explorer les moyens d'adapter les lois et règlements en vigueur protégeant les enfants en ligne dans l'environnement mobile. Ainsi, aux États-Unis, des lois fédérales limitent le recueil, l'utilisation et la communication d'informations potentiellement nominatives émanant ou concernant des enfants de moins de 13 ans dans les services en ligne. Elles prévoient notamment une

information sur les politiques en matière de vie privée, la vérification de l'accord parental pour le recueil d'informations nominatives auprès des enfants (avec un certain nombre d'exceptions limitées), la vérification et la suppression par les parents des données personnelles émanant de leurs enfants et l'obligation de procédures destinées à protéger la sécurité des données.

Surconsommation de services offerts via des téléphones portables

Certains pays sont allés beaucoup plus loin, en responsabilisant davantage les opérateurs mobiles. En Finlande, le Bureau des plaintes de consommation a établi la responsabilité des prestataires de services dans une affaire concernant des jeux télévisés fondés sur une participation par SMS. Il a ainsi été constaté que l'opérateur mobile avait perçu des gains indus. Le fait qu'un parent ait autorisé son enfant à utiliser le téléphone parental ne constituait pas en soi une autorisation pour l'enfant de s'engager légalement dans une transaction commerciale telle que le jeu télévisé en question. En vertu de cette décision, le consommateur était fondé à demander un remboursement.

Marketing en direction des enfants

Les *Lignes directrices sur le commerce électronique* recommandent que les entreprises prennent un soin tout particulier dans la publicité et le marketing en direction des enfants dans la mesure où ceux-ci peuvent ne pas avoir la capacité de comprendre pleinement l'information qui leur est présentée. De la même manière, les lignes directrices de la MMA *(paragraphe* 4.0) indiquent que le fait de proposer « en direction des enfants des programmes qui font la promotion ou incitent à la consommation de contenus numériques de toute nature fait intervenir d'importantes considérations en matière d'éthique, de responsabilité et de sensibilité, que tous les participants du secteur sont appelés à prendre en compte ». Bien que certains pays disposent de lois ou de réglementations limitant ce type de marketing, ils sont peu nombreux à avoir des dispositions visant spécifiquement le commerce mobile. L'un des rares dans ce cas est le Royaume-Uni, où les publicités pour des produits de restauration rapide en direction des enfants sont interdites sur les téléphones portables.

L'édition américaine des Lignes directrices du MMA pour les messages SMS et MMS à destination des enfants de moins de 13 ans (voir le para. 4.0) invite tous les participants du secteur de la téléphonie mobile à préciser dans tous les messages publicitaires visuels ou sonores que le service est surtaxé (le cas échéant), le montant précis facturé et, s'il y a lieu, le fait que s'ajoute aussi le prix de la communication. Les Lignes directrices indiquent également que le terme « gratuit » ne peut être utilisé, à moins qu'aucun droit ou aucune charge ne soit associé au service.

En Finlande, la *Loi sur les services de tutelle* stipule que les mineurs ne peuvent effectuer que des transactions habituelles pour leur âge et de faible montant. Aux termes de la *Loi finlandaise sur le marché des communications*, l'Autorité finlandaise de régulation des communications définit *certaines catégories de services interdites dans les télécommunications*. Les abonnés, par exemple les parents, peuvent

déterminer eux-mêmes les types de services surtaxés qu'ils veulent bloquer pour les appels téléphoniques ou SMS. Le fait d'interdire une catégorie de services bloque tous les services appartenant à la catégorie en question. Le Médiateur des consommateurs a également négocié certaines améliorations en ce qui concerne la situation des mineurs abonnés à des services mobiles et il a coopéré avec les professionnels dans ce sens. L'attention des responsables de réseaux a été attirée sur les responsabilités qui leur incombaient quant aux systèmes qu'ils utilisent et sur l'obligation de respecter la législation en vigueur. Le Médiateur des consommateurs a également attiré l'attention des opérateurs mobiles sur leurs responsabilités en tant qu'entité de facturation, notamment pour le traitement des plaintes et l'indemnisation, le cas échéant.

Utilisation non autorisée des téléphones portables

En Finlande, la question de l'identification de la partie contractante a été examinée. Le Ministère de la justice a par exemple mis en place un groupe de travail pour rédiger un projet de loi modifiant la législation sur les prêts immédiats par SMS. L'identification du consommateur ne repose actuellement que sur l'information relative à l'abonnement mobile et le numéro de sécurité sociale. Le groupe de travail va examiner s'il conviendrait d'imposer statutairement aux organismes prêteurs d'identifier de façon plus fiable les clients.

Considérations liées à la vie privée

La *Loi finlandaise sur la protection de la vie privée dans les communications électroniques* impose d'obtenir l'autorisation des consommateurs avant que ceux-ci puissent recevoir des messages électroniques de marketing direct. Le Médiateur à la protection des données et l'Agence de défense des consommateurs/le Médiateur des consommateurs ont par exemple élaboré des Principes directeurs sur les pratiques de marketing dites « de parrainage », qui précisent que l'autorisation préalable du destinataire doit être obtenue et stipulent les cas dans lesquels cela n'est pas nécessaire (on parle de marketing de parrainage quand un consommateur retransmet à des personnes de sa connaissance, par courrier électronique ou SMS, des offres privilégiées, des conseils d'utilisation de produits, des invitations à des concours ou d'autres messages de marketing).

La *Loi finlandaise sur la protection de la vie privée dans les communications électroniques* couvre également la confidentialité des données d'identification et de localisation. Elle prévoit notamment des limitations du traitement des données d'identification, à des fins de marketing par exemple, ainsi que des limitations du traitement et de la communication des informations de localisation. De même, la personne à localiser doit avoir donné expressément son consentement à ce type de service. S'agissant des mineurs de moins de 15 ans, c'est au tuteur qu'incombe la responsabilité de décider au sujet du traitement des données de localisation.

Aux États-Unis, la possibilité dont dispose un opérateur de communiquer à des tiers des informations de géolocalisation relatives aux abonnés est limitée par les dispositions statutaires relatives à l'utilisation des informations de réseau propriétaires concernant la clientèle (Customer Proprietary Network information

ou « CPNI »). Ainsi, l'article 222 de la Loi fédérale sur les communications interdit la communication ou l'utilisation des informations de localisation de terminaux sans fil, obtenues par un opérateur dans le cadre de sa prestation de services de télécommunications, sans le consentement préalable expresse de l'abonné, sauf dans des situations d'urgence particulières afin de permettre de répondre à un appel d'urgence d'un abonné sans fil ou en liaison avec la transmission automatiquement de données lors d'un accident. De plus, la Loi « CAN SPAM » (Controlling the Assault of Non-Sollicited Pornography and Marketing) interdit l'envoi de messages commerciaux de service mobile directement sur des terminaux sans fil via l'Internet sans l'autorisation préalable expresse du destinataire. En outre, aux États-Unis la Loi « TCPA » (Telephone Consumer Protection Act) interdit tout appel émis au moyen d'un système de composition téléphonique automatique ou d'un message synthétique ou préenregistré à destination de tout numéro de téléphone mobile, qu'il s'agisse d'appels vocaux ou de messages textuels.

Appendice I.2
INSTRUMENTS DE L'OCDE AYANT TRAIT AUX QUESTIONS DE COMMERCE MOBILE

Instruments de protection des consommateurs

- Lignes directrices de l'OCDE de 1999 régissant la protection des consommateurs dans le contexte du commerce électronique.
- Lignes directrices de l'OCDE de 2003 régissant la protection du consommateur contre les pratiques transfrontières commerciales frauduleuses et trompeuses (OCDE, 2003), qui définissent un cadre pour la lutte contre toutes les sortes d'activités frauduleuses en ligne et hors ligne, au niveau tant national qu'international.
- *Recommandation de l'OCDE de 2007 sur le règlement des litiges de consommation et leur réparation* (OCDE, 2007c), qui vise à offrir aux consommateurs des mécanismes efficaces pour le règlement de leurs litiges et l'obtention de réparations, que se soit au niveau intérieur ou transfrontière.
- Projet d'Orientation d'action de l'OCDE de 2008 sur le vol d'identité en ligne.

Instruments relatifs à la sécurité, la vie privée et la lutte contre le Spam

- *Lignes directrices de l'OCDE de 2002 régissant la sécurité des systèmes et réseaux d'information* (OCDE, 2002), qui énoncent des principes assurant des approches nationales homogènes pour la prise en compte des risques de sécurité dans une société interconnectée au niveau planétaire.
- *Recommandation de l'OCDE de 2007 et Principes directeurs relatifs à l'authentification électronique* (OCDE 2007d), Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.
- Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (OCDE, 1980), qui contiennent des principes sur le recueil et le traitement des données de caractère personnel.
- *Recommandation de l'OCDE de 2007 sur la coopération transfrontière dans l'application des législations protégeant la vie privée* (OCDE, 2007e), qui invite les autorités des pays membres à coopérer avec les autorités étrangères et à s'entre-aider dans l'application des législations sur la vie privée.
- *Boîte à outils de l'OCDE* 2006 de politiques et mesures recommandées pour la lutte contre le Spam, qui vise à faciliter la coopération internationale dans la lutte contre le spam et propose une série de recommandations pour mettre en place des politiques complémentaires dans l'application des initiatives antispam entre pays membres de l'OCDE.

BIBLIOGRAPHIE

CE (Commission européenne) (2006), *Eurobaromètre spécial pour un Internet plus sûr*, mai 2006, http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.

CE (2007), *12ème Rapport de la Commission sur la régulation et les marchés des communications électroniques en Europe*, COM(2007)155, 29 mars 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0155:FR:HTML .

OCDE (Organisation de coopération et de développement économiques) (1980), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* OCDE, Paris, http://www.oecd.org/document/18/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html.

OCDE (1999), *Recommandation du Conseil relative aux lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*, OCDE, Paris, www.oecd.org/dataoecd/17/59/34023530.pdf

OCDE (2002), *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*, OCDE, Paris, http://www.oecd.org/dataoecd/16/22/15582260.pdf

OCDE (2003), *Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, OCDE, Paris, http://www.oecd.org/dataoecd/24/33/2956464.pdf .

OCDE (2006), *Boîte à outils antispam, politiques et mesures recommandées*, OCDE, Paris, www.oecd-antispam.org/.

OCDE (2007a), *Le commerce mobile*, DSTI/CP(2006)7/FINAL, www.oecd.org/dataoecd/46/39/38087511.pdf .

OCDE (2007b), *Perspectives des communications de l'OCDE 2007*, OCDE, Paris, http://213.253.134.43/oecd/pdfs/browseit/9307022E.PDF.

OCDE (2007c), *Recommandation sur le règlement des litiges de consommation et leur réparation*, OCDE, Paris, http://www.oecd.org/dataoecd/43/49/38960185.pdf.

OCDE (2007d), *Recommandation de l'OCDE de 2007 et Principes directeurs relatifs à l'authentification électronique*, OCDE, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf

OCDE (2007e), *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie*, OCDE, Paris, http://www.oecd.org/dataoecd/12/48/38876531.pdf.

UIT (Union internationale des télécommunications) (2004), *Mobile phones and youth, a look at the US student market*, février 2004, www.itu.int/osg/spu/ni/futuremobile/Youth.pdf.