Lignes directrices sur la protection en ligne des enfants à l'intention des décideurs

www.itu.int/cop

REMERCIEMENTS

Les présentes lignes directrices ont été élaborées par l'Union internationale des télécommunications (UIT) avec le concours d'une équipe d'auteurs collaborateurs issus des principales organisations actives dans le secteur des technologies de l'information et de la communication (TIC) et traitant des questions liées à la sécurité des enfants dans le cyberespace. Leur établissement n'aurait pas été possible sans l'engagement et l'enthousiasme de ces auteurs collaborateurs.

L'UIT remercie les auteurs énumérés ci-après (par ordre alphabétique) pour leur précieuse contribution en temps et en réflexion:

- Cristina Bueti et Sandra Pandi (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Raoul Chiesa et Francesca Bosco (Institut interrégional de recherche des Nations Unies sur la criminalité et la justice)
- Catherine Cummings et Jessica Sarra (*International Centre for Missing & Exploited Children*)
- Johan Martens (*Child Helpline International*)
- Michael Moran (Interpol)

Les auteurs tiennent également à remercier Kristin Kvigne (Interpol) pour son analyse et ses commentaires détaillés.

L'UIT souhaite honorer Salma Abbasi d'eWWG pour sa profonde implication dans le cadre de l'initiative pour la protection en ligne des enfants (COP).

Des informations complémentaires et autres ressources concernant le projet de lignes directrices peuvent être consultées à l'adresse http://www.itu.int/cop. Ces données font l'objet d'une actualisation régulière.

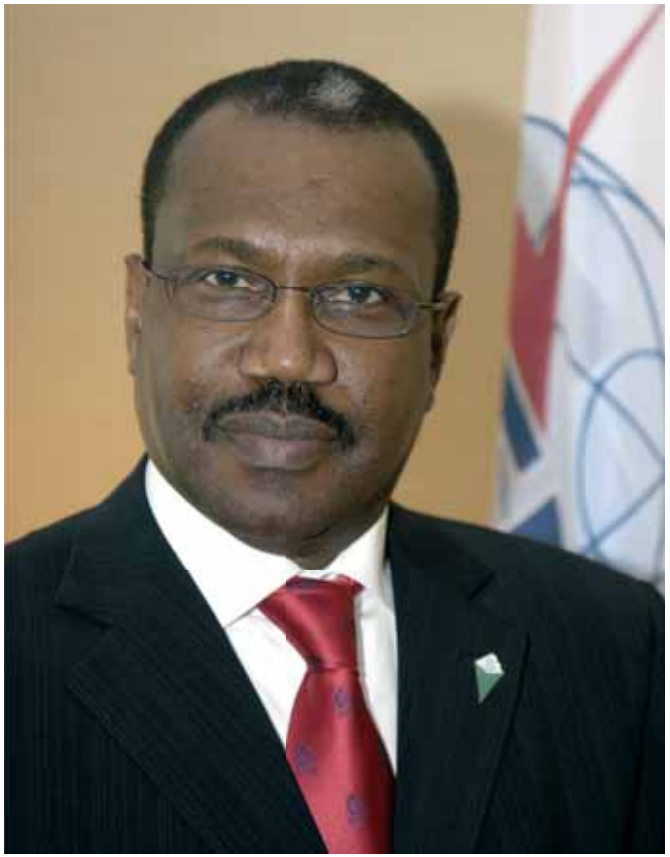
Les lecteurs qui auraient des commentaires à faire ou des informations supplémentaires à fournir sont invités à contacter cop@itu.int

Table des matières

Crédit photos: www.shutterstock.com, Violaine Martin/UIT, Ahone Ayeh Njume-Ebong/UIT


«La protection en ligne des enfants est une problématique mondiale qui nécessite une réponse mondiale»

Avant-propos



J'ai le plaisir de vous présenter ces lignes directrices qui ont été élaborées avec le précieux concours de différents acteurs.

La protection en ligne des enfants – alors que l'Internet à large bande est de plus en plus accessible – représente un défi majeur qui requiert l'application immédiate d'une solution mondiale coordonnée. Les initiatives locales voire nationales sont certes efficaces, mais l'Internet ne connaît pas de frontières et seule la conjugaison de nos efforts au niveau international nous permettra d'assurer un avenir plus sûr pour nos enfants.

Vous jouez, en votre qualité de décideur, un rôle clé dans la lutte contre la cybercriminalité et les cybermenaces et je tiens à vous remercier personnellement de votre soutien.

Dr Hamadoun I. Touré
Secrétaire général de l'Union internationale des télécommunications (UIT)

Aux termes de la Convention des Nations Unies sur les droits de l'enfant, est considérée comme «enfant» toute personne âgée de moins de 18 ans. Les présentes lignes directrices sont destinées à répondre aux problématiques qui touchent toutes les personnes âgées de moins de 18 ans dans toutes les régions du monde. Cependant, l'internaute de 7 ans n'aura pas les mêmes besoins ni les mêmes centres d'intérêt que le jeune de 12 ans qui entame sa scolarité ou que l'adolescent de 17 ans à l'aube de sa majorité. Aussi, ces lignes directrices fournissent-elles à plusieurs reprises des conseils et des recommandations ciblés en fonction de la situation. Si l'utilisation de catégories générales peut s'avérer particulièrement utile, il n'en demeure pas moins que chaque enfant est et reste différent. Qui plus est, l'utilisation ou l'interprétation de ces lignes directrices dans un pays ou une région donnés peuvent considérablement varier selon les facteurs locaux juridiques et culturels.

Il existe aujourd'hui un corps imposant de règles internationales et d'instruments internationaux qui sous-tendent et bien souvent prescrivent les mesures visant à protéger les enfants, de manière générale et plus spécifiquement en relation avec l'Internet. Ces règles et ces instruments constituent la base des présentes lignes directrices. Ils sont répertoriés de manière exhaustive dans la Déclaration et l'Appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents, adoptés lors du Troisième congrès mondial contre l'exploitation sexuelle des enfants et des adolescents en novembre 2008.

Résumé analytique

Il y a dix ans, on comptait dans le monde à peine 182 millions d'internautes, et presque tous vivaient dans les pays développés. Au début de 2009, ce nombre était passé à 1,5 milliard et plus de 400 millions des utilisateurs avaient accès à la large bande. Aujourd'hui, avec plus de 600 millions d'utilisateurs en Asie, 130 millions en Amérique latine et dans les Caraïbes et 50 millions en Afrique[1] l'Internet – bien que non encore omniprésent – constitue une ressource dynamique incroyable aux possibilités quasi infinies, capable de répondre aux grandes problématiques de la société (meilleur accès aux soins de santé, apprentissage en ligne, services de cybergouvernement, postes innovants et comportant une rémunération plus élevée, etc.). Toutefois, les risques liés à la cybersécurité ne cessent de croître au niveau mondial et requièrent une action internationale, en particulier lorsqu'il s'agit de protéger nos citoyens les plus jeunes et les plus vulnérables que sont nos enfants.

Selon des enquêtes récentes, plus de 60% des enfants et des adolescents discutent chaque jour sur l'Internet sur des sites de «chat». Trois enfants sur quatre en ligne se disent prêts à révéler des informations personnelles sur eux-mêmes et sur leur famille en échange de biens et de services. Et un enfant sur cinq sera chaque année la proie d'un prédateur.

Ces lignes directrices ont été mises au point dans le cadre de l'Initiative pour la protection en ligne des enfants (COP)[2] visant à créer les conditions nécessaires à l'instauration d'un univers en ligne sûr et sans danger pour les générations futures. Elles ont été conçues pour servir de plan directeur, lequel peut être adapté et utilisé dans le respect des règles et des coutumes nationales ou locales. Il est également souhaité que la présente publication traite de thématiques touchant tous les enfants et adolescents de moins de 18 ans, même si les besoins ne sont pas les mêmes pour chaque groupe d'âge.

Ces lignes directrices ont été élaborées par l'UIT en collaboration étroite avec une équipe d'auteurs collaborateurs issus des principales institutions actives dans le secteur des TIC et traitant de questions liées à la sécurité en ligne des enfants: *Children's Charities' Coalition on Internet Safety* (CHIS), *Child Helpline International* (CHI), *International Centre for Missing & Exploited Children (ICMEC)*, Interpol et l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI). Certains gouvernements nationaux et sociétés high-tech qui ont pour objectif commun de faire

[1] World Telecommunication/ICT Indicators Database 2008, 12th Edition.

[2] www.itu.int/cop

de l'Internet un lieu sûr et sans danger pour les enfants et les adolescents ont également apporté une contribution précieuse.

Ces lignes directrices devraient favoriser l'édification d'une société de l'information plus inclusive, mais permettre également aux Etats Membres de l'UIT de satisfaire aux obligations souscrites pour protéger et concrétiser les droits des enfants tels qu'ils sont énoncés dans la Convention des Nations Unies sur les droits de l'enfant[3], adoptée par l'Assemblée générale des Nations Unies aux termes de sa Résolution 44/25 du 20 novembre 1989 et dans le document final[4] du Sommet mondial sur la société de l'information[5] (SMSI).

Au SMSI, l'UIT s'est vu confier par les dirigeants de la communauté internationale la responsabilité de la grande orientation C5 («Etablir la confiance et la sécurité dans l'utilisation des TIC»). Les documents du SMSI reconnaissent spécifiquement les besoins des enfants et des adolescents et la nécessité de les protéger dans le cyberespace. L'Engagement de Tunis reconnaît «le rôle des technologies de l'information et de la communication (TIC) dans la protection et le développement des enfants» ainsi que la nécessité «de renforcer les mesures destinées à protéger les enfants contre tout abus et à assurer la défense de leurs droits dans le contexte des TIC».

Par la publication de ces lignes directrices, l'Initiative COP appelle toutes les parties prenantes à promouvoir l'adoption de politiques et de stratégies susceptibles de protéger les enfants dans le cyberespace et à promouvoir leur accès en toute sécurité à l'Internet et à ses ressources considérables.

[3] www.unicef.org/crc/

[4] Le SMSI a été conçu en deux phases: l'une à Genève (du 10 au 12 décembre 2003), l'autre à Tunis (du 16 au 18 novembre 2005). Les participants au SMSI ont réaffirmé leur détermination «d'édifier une société à dimension humaine, inclusive et privilégiant le développement, une société de l'information, dans laquelle chacun ait la possibilité de créer, d'obtenir, d'utiliser et de partager l'information et le savoir». Voir www.itu.int/wsis

[5] www.itu.int/wsis

Lignes directrices à l'intention des décideurs

Les décideurs peuvent adopter plusieurs stratégies en vue de développer une politique nationale relative à la sécurité des enfants dans le cyberespace. Le tableau ci-dessous présente certains paramètres à prendre en compte. D'autres pistes sont également suggérées à l'Appendice 4.

	#	Paramètres à prendre en compte
Cadre juridique	1.	Analyser le cadre juridique existant pour repérer la présence des mécanismes juridiques d'application de la loi et permettre aux autres organismes compétents de protéger les personnes de moins de 18 ans sur toutes les plates-formes connectées à l'Internet.
	2.	Etablir, *mutatis mutandis*, que tout acte commis sur un enfant qui s'avère illégal dans le monde réel est tout aussi illégal dans le cybermonde et que les règles sur la protection des données et de la vie privée dans le cyberespace s'appliquent également aux mineurs.
Ressources nécessaires à l'application de la loi et outils de signalement	3.	Veiller à l'établissement et à la promotion à large échelle d'un outil de signalement des contenus illicites trouvés sur l'Internet (par exemple, une hotline nationale capable de fournir une réponse rapide, de supprimer les ressources illicites ou de les rendre inaccessibles).

	#	Paramètres à prendre en compte
Action nationale	4.	Rassembler l'ensemble des intervenants qui se préoccupent de la sécurité en ligne des enfants, en particulier: • les organismes gouvernementaux • les organismes chargés de l'application de la loi • les organismes de services sociaux • les fournisseurs d'accès à Internet (FAI) et autres fournisseurs de services électroniques • les exploitants de réseau de téléphonie mobile • d'autres sociétés de haute technologie • les organisations de professeurs • les organisations de parents d'élèves • les enfants et les adolescents • les agences de protection de l'enfance et autres ONG compétentes • le monde de l'enseignement et de la recherche • les propriétaires de cybercafés et autres fournisseurs d'accès public (bibliothèques, télécentres, PC Bangs[6], salles de jeux en réseau, etc.).
	5.	Considérer les avantages d'un modèle d'autoréglementation ou de coréglementation en matière de développement de la politique, comme en témoignent l'élaboration et la publication du code de bonnes pratiques, tant en termes de stimulation et de soutien des parties prenantes concernées qu'en termes de rapidité de formulation et de mise en application des mesures adoptées en réponse aux mutations technologiques.
Moyens d'enseignement et de sensibilisation	6.	Renforcer le savoir et l'expérience de toutes les parties prenantes et élaborer des messages et des supports d'information sur la sécurité sur Internet qui soient conformes aux normes et règles culturelles locales et qui présentent la garantie d'une distribution efficace et d'une diffusion appropriée auprès du public cible visé. Faire appel, le cas échéant, aux médias de masse pour véhiculer les messages de sensibilisation. Mettre au point une documentation qui présente les aspects positifs et stimulants de l'Internet pour les enfants et les adolescents et proscrit tout message alarmant. Encourager un comportement en ligne positif et responsable.
	7.	Etudier le rôle que peuvent jouer les outils techniques, tels que les programmes de filtrage et les logiciels de sécurité enfants, en marge et en complément des initiatives d'enseignement et de sensibilisation.
	8.	Encourager les utilisateurs à être responsables de leur ordinateur, en assurant un entretien courant lequel inclut la mise à jour du système d'exploitation ainsi que l'installation et la mise à niveau d'un pare-feu et d'un antivirus.

[6] Un «PC Bang» est un terme couramment utilisé en Corée du Sud et dans d'autres pays pour désigner une grande salle équipée d'installations LAN permettant de jouer en réseau, avec d'autres internautes ou avec les joueurs en présence dans la salle.

1. Considérations générales

La technologie que nous appelons aujourd'hui «l'Internet» remonte aux années 50, voire avant. Mais c'est surtout avec l'avènement du *World Wide Web*, au début des années 90, que l'Internet a connu une croissance exponentielle jusqu'à devenir une ressource extrêmement précieuse de notre quotidien, sur le plan tant économique que social, de même qu'un élément visiblement incontournable de la vie moderne.

A l'aube de la révolution Internet, les utilisateurs s'émerveillaient de pouvoir, en deux trois clics de souris, communiquer et échanger des informations par delà les océans et les fuseaux horaires. Ils étaient néanmoins tributaires d'un équipement informatique fixe et souvent encombrant appelé PC. Aujourd'hui, il est possible de se connecter au réseau mondial par le biais d'un téléphone portable, d'un notebook ou d'un autre terminal nomade et de bénéficier de surcroît de fonctions vidéo et d'un accès ultrarapide. De nombreuses consoles de jeu intègrent également une connexion Internet, ce qui a considérablement dopé le marché des jeux en ligne à destination des enfants et des adolescents.

Il a fallu près de 20 ans pour que le nombre d'abonnés à la téléphonie mobile totalise 1 milliard. Ce chiffre a atteint deux milliards rien qu'au cours des dernières années. Par comparaison, il a fallu attendre 125 ans pour que le nombre d'usagers de la téléphonie fixe dépasse le milliard.

Le passage de la deuxième à la troisième génération de réseaux mobiles semble constituer une étape tout aussi importante que le fut la transition de l'analogique au numérique. Le processus, enclenché il y a une dizaine d'années, progresse rapidement.

« Rassembler l'ensemble des intervenants qui se préoccupent de la sécurité en ligne des enfants »

Les technologies de quatrième génération nouvellement émergentes se concentrent toujours sur l'accès mobile mais à des vitesses toujours plus grandes. Les réseaux à large bande et la convergence des médias ouvrent de nouvelles perspectives en matière de diffusion des divertissements numériques.

Les équipements d'utilisateur sont aujourd'hui multifonctions et de plus en plus personnalisés. Des centaines de millions de terminaux pourront bientôt communiquer entre eux via Internet et ouvrir d'innombrables applications domestiques et commerciales.

Que ce soit sur le marché de la téléphonie fixe ou sur le marché de la téléphonie mobile cellulaire, la transition vers des réseaux de capacité supérieure ne peut se faire sans un basculement vers les réseaux IP. L'utilisation du protocole VoIP (*Voice over Internet Protocol*) devient par conséquent de plus en plus répandue (par exemple grâce à des services comme Skype ou Vonage), de même que la possibilité de visionner des images en mouvement sur les réseaux IP. Avec l'essor des nouvelles technologies que sont notamment la radiodiffusion vidéonumérique et la radiodiffusion multimédia numérique, la lecture continue de contenus sur des terminaux mobiles sera bientôt possible à tout moment et en tous lieux.

Le monde du divertissement semble entrer dans une toute nouvelle ère. Dans le même temps, la technologie numérique modifie en profondeur la nature des interactions sociales. Le téléphone mobile a déjà changé notre façon de communiquer, d'organiser des rencontres et de traiter plusieurs tâches simultanément.

Grâce au développement des infrastructures électroniques et numériques, plusieurs millions de personnes peuvent désormais s'informer, publier et communiquer de façon entièrement novatrice. Les enfants et les adolescents sont souvent les «pionniers» qui adoptent et utilisent les possibilités offertes par les technologies émergentes. Face à de nouvelles opportunités en matière d'éducation et d'apprentissage personnalisé, de nombreux jeunes voient dans cette évolution un défi particulièrement excitant.

Compte tenu de la baisse rapide des coûts réels des technologies de l'information et de la communication ainsi que des importantes mutations et améliorations apportées aux infrastructures disponibles, nombre d'enfants et d'adolescents peuvent aujourd'hui se servir de la technologie pour concevoir et réaliser des projets restés inconnus des générations antérieures.

L'Internet n'affiche pas le même stade de développement selon les pays et les régions, mais il est possible de s'y connecter depuis les quatre coins de la planète. Dans les pays en développement, les connexions Internet et téléphonique utilisent principalement la technologie sans fil et ne passent pas par une ligne fixe. Le stockage et le transfert des données sont de plus en plus décentralisés et quasi illimités. La «société en réseaux» (*networked society*) telle qu'envisagée il y a quelques dizaines d'années devient donc réalité.

De plus en plus accessible, l'Internet est partout et profite à un nombre toujours plus grand de personnes, y compris aux enfants et aux adolescents. Le développement du réseau mondial diffère selon la culture et l'économie du pays. Les risques auxquels sont confrontés les enfants ne sont donc pas les mêmes. Et la façon dont les différents acteurs locaux entendent gérer ces risques n'est donc pas la même. Force est de constater qu'il n'existe pas une seule et unique manière de traiter une question aussi complexe.

2. Utilisation de l'Internet par les enfants et les adolescents

Si l'Internet existe depuis plusieurs décennies, force est de constater que la nature du réseau a considérablement évolué depuis ses débuts. Au départ, il s'agissait essentiellement d'un outil permettant aux agences gouvernementales et aux institutions universitaires d'échanger entre elles des informations et des données. Au cours des années 80, le réseau a été ouvert au grand public puis a connu une croissance fulgurante à partir des années 90 avec l'avènement du *World Wide Web*. Une autre révolution a eu lieu ces dernières années avec l'arrivée du Web 2.0. Le web devient de plus en plus interactif et ses utilisateurs sont de plus en plus nombreux dans le monde. On enregistre une augmentation du taux de connexion, en particulier chez les enfants et les adolescents qui sont très souvent les premiers utilisateurs.

Bien qu'il ait été rendu accessible au grand public, l'Internet a conservé assez longtemps l'image d'un réseau ayant été détenu et fréquenté principalement par les gouvernements, les institutions universitaires et les sociétés commerciales. Les particuliers se connectaient surtout dans le but d'obtenir des informations mises à leur disposition par ces mêmes acteurs. Cette version initiale du web se caractérise par les aspects suivants:

- faibles niveaux de connectivité
- largeur de bande relativement petite

form
little
traditional
crafts
term
example
public's
capabilities
store
government
corporation
wide
using
world
network
ipv6
interoperable
servers
global
lagging
influence
may
systems
graphics
interactive
infrastructure
generally
local
databases
blogs
find
standardized
connection
physical
data
access
web
series
interconnection
brand
discussions
communications
content
groups
terms
synonymous
strict
widely
management
implementations
files
lan
internet
applied
food
communities
encyclopedias
growth
maintaining
areas
standardization
controlling
progressed
logs

- faible capacité de stockage des données
- communication et accès en mode unidirectionnel

L'Internet s'est ensuite progressivement développé autour de quatre axes majeurs:

- extension de la largeur de bande à prix abordable
- augmentation de la capacité de stockage relativement bon marché
- diminution des coûts d'accès
- développement de l'Internet mobile

Ces évolutions ont contribué à l'émergence d'un Internet d'un genre nouveau qui, au lieu de simplement mettre en relation les individus avec les sociétés, les organisations et les gouvernements, a commencé à permettre aux particuliers de se connecter les uns aux autres et d'émettre eux-mêmes des publications. Cette nouvelle mouture d'Internet, connue sous le nom de Web 2.0, présente les caractéristiques suivantes:

- forts niveaux de connectivité
- largeur de bande élevée
- importante capacité de stockage
- contact personnalisé et interactif (contenu généré par l'utilisateur)

Des outils de socialisation et de mise en relation, tels que la messagerie instantanée, les sites de chat et babillards électroniques, les services d'hébergement de photos et de vidéos et les programmes d'échange de fichiers entre homologues (P2P), ont été développés à l'intention des utilisateurs. Ces diverses technologies ont permis la croissance fulgurante des sites de réseautage social qui, en très peu de temps, ont acquis une immense popularité auprès des jeunes.

Interactivité et contenu généré par l'utilisateur

Les enfants et les adolescents de même que les adultes ont aujourd'hui de plus en plus recours à ces nouvelles technologies dans leur quotidien, et la nature des risques auxquels ils sont confrontés devient de fait inextricablement liée à certains aspects plus larges de leur comportement. Il n'existe plus de démarcation nette entre les «problématiques Internet» et les problèmes du «monde réel».

Sites de réseautage social

Les sites de réseautage social doivent leur succès et leur attrait à leur capacité de rassembler plusieurs technologies Internet préexistantes en un seul endroit, d'insérer de nouvelles fonctionnalités et de créer des interfaces ultraconviviales qui simplifient considérablement l'utilisation de ces nouvelles fonctionnalités. Tout cela a contribué à accroître rapidement la popularité des sites de socialisation qui surprennent et séduisent de nombreuses personnes, à commencer par les parents.

Pour se connecter à un site de réseautage social, l'utilisateur doit créer son profil en ligne et renseigner un certain nombre d'informations personnelles (âge, sexe, lieu de résidence, centres d'intérêt, etc.). Il peut facilement personnaliser ses propres pages web, par le biais des nouvelles interfaces créées pour ces sites, en ajoutant par exemple ses musiques, ses photos ou ses vidéos préférées. Les enfants et les adolescents font preuve d'une très grande créativité dans cet exercice. Leur profil d'utilisateur sur les sites

de réseautage social devient une extension de leur personnalité et un puissant outil leur permettant de se dévoiler à leurs amis et au monde entier.

Plus important encore, les sites de réseautage social permettent aux utilisateurs de se faire de nouveaux amis avec qui échanger des messages. La possibilité de pouvoir consulter ou non le profil d'un utilisateur dépend des paramètres de confidentialité définis par l'utilisateur en question. Trop souvent, et notamment au début de l'utilisation de ces sites, les enfants et les adolescents ne semblaient pas être au courant du fait que n'importe qui pouvait consulter les informations personnelles de leur profil s'ils ne définissaient pas certains paramètres pour en limiter l'accès (par exemple, en sélectionnant «Privé» ou «Seulement mes amis»). Ils étaient ainsi exposés aux prédateurs qui masquaient souvent leur âge pour entrer en relation avec les jeunes utilisateurs. Il a été rapporté que des enfants et des adolescents publiaient en ligne ou échangeaient via le téléphone mobile des images d'eux-mêmes à caractère sexuel – phénomène connu sous le nom de «sexting»[7] – sans savoir bien souvent que ces images peuvent être illicites et leur être préjudiciables, mais surtout sans réaliser que de nombreuses personnes peuvent consulter leur site ou leur profil et ainsi accéder ainsi à ces images. De manière plus générale, les sites de réseautage social ont été confrontés au problème de la gestion des contenus générés par l'utilisateur qui sont l'apanage du Web 2.0. Certains sites ont développé des politiques de modération et traquent toute vidéo ou image indécente ou illégale, tandis que d'autres ne se pencheront sur une image ou une vidéo en particulier que si cette dernière est portée à leur attention dans le cadre d'un rapport établi par une personne qui la juge inopportune et demande sa suppression.

La popularité des sites sociaux est souvent fonction de la langue utilisée et de facteurs régionaux. Prenons l'exemple de MySpace (particulièrement populaire en Amérique du Nord), de Facebook (plus populaire en Amérique du Nord, en Europe et en Océanie), de Hi5 (plus populaire en Amérique latine), d'Orkut (Amérique latine), de SkyBlog (pays francophones), de Live Journal (Russie et CEI), de Friendster (Asie-Pacifique), de Cyworld (République de Corée et République populaire de Chine), de LinkedIn (Europe, Etats-Unis et Inde) et de Last.fm (pays nordiques et pays baltes, Europe centrale).

[7] «Sexting»: phénomène relativement nouveau qui consiste, pour des enfants ou des adolescents, à s'exposer à des risques, en diffusant en ligne des photos provocantes d'eux-mêmes ou en les envoyant à des amis au moyen de technologies mobiles.

Source: Projets de lignes directrices sur la protection de l'enfance en ligne à l'intention des parents, des tuteurs et des éducateurs, UIT, 2009.

Selon Danah Boyd[8], les commentaires en ligne, profils d'utilisateur et autres types de publication sur le net présentent quatre caractéristiques fondamentales qui peuvent entraîner des risques supplémentaires pour les enfants et les adolescents:

1. Persistance: les communications en réseau sont enregistrées, ce qui prolonge la durée de vie des informations échangées.

2. Capacité à être recherché/retrouvé: parce que les communications en ligne sont enregistrées et parce qu'il est possible d'établir une identité au travers du texte, des personnes peuvent retrouver d'autres personnes au moyen des moteurs de recherche.

3. Reproductibilité: les communications en réseau peuvent être copiées textuellement d'un endroit à l'autre, de sorte qu'il devient impossible de distinguer l'«original» de la «copie».

4. Audiences invisibles: pour des raisons pratiques, il est impossible de savoir qui consulte les profils et autres communications en ligne. La conjugaison des trois critères précédemment cités complique encore la chose, puisqu'un profil peut être visité à un moment et à un endroit qui ne sont pas ceux où il a été créé initialement.

Messagerie instantanée et chat

Les outils de messagerie instantanée (MI) offrent la possibilité de se connecter directement les uns aux autres et de converser en ligne au moyen de messages écrits (et de plus en plus par vidéoconférence). En créant une liste de contacts, les utilisateurs savent si leurs amis sont disponibles (en ligne) pour discuter. Ces conversations ou «chats» peuvent être menés avec une seule personne (sur une base unilatérale) ou avec un groupe de personnes (sur une base multilatérale). La majorité des programmes permettent de sauvegarder le contenu des conversations si nécessaire ou si souhaité. Les programmes de MI et de chat les plus connus sont MSN Chat, Yahoo! Messenger, Google Talk et AOL Instant Messenger.

Programmes d'échange de fichiers entre homologues

Les programmes d'échange de fichiers entre homologues (programmes P2P) permettent aux utilisateurs de télécharger directement des fichiers depuis et vers leurs propres disques de stockage. A partir du moment où le même programme est utilisé, un utilisateur peut rechercher et télécharger des fichiers chez les autres utilisateurs disposant de ces fichiers. S'ils favorisent le partage du savoir et de l'information, ces programmes peuvent aussi entraîner des violations de droits d'auteur et la prolifération de virus malveillants (*malware*) tels que les virus et les chevaux de Troie[9]. Ces réseaux sont également utilisés pour la diffusion du matériel pédopornographique. On recense au nombre des principaux programmes P2P: Bittorent, E-mule, E-donkey et Kazaa.

[8] Danah Boyd est membre du *Harvard Law School's Berkman Center for Internet and Society*.

[9] Le cheval de **Troie** ou Trojan (informatique) est un type de programme malveillant (*malware*) qui, en apparence, semble exécuter des actions légitimes mais qui, de manière larvée, exécute des actions préjudiciables qui permettent un accès non autorisé à l'hôte dans le but de sauvegarder des fichiers sur la machine de l'utilisateur voire de visualiser l'écran et de prendre le contrôle de la machine. Voir: http://en.wikipedia.org/wiki/Trojan_horse_(computing)

3. Matériel pédoporno-graphique

Définition

Dans de nombreuses juridictions, les photographies ou vidéos d'enfants exploités sexuellement sont qualifiées de «pornographie enfantine» ou d'«images indécentes d'enfants». Nombre de praticiens parlent aujourd'hui plus volontiers de «matériel pédopornographique» qui, selon eux, correspond plus précisément à la nature réelle du contenu. Tel est le terme que nous avons choisi d'utiliser dans le présent document.

L'Internet a radicalement modifié l'échelle et la nature de la production et de la diffusion du matériel pédopornographique.

La révolution sexuelle arrivée dans le milieu des années 60 et marquée par le développement d'une culture d'ouverture autour de l'orientation sexuelle a ouvert une brèche en matière de pornographie, et les librairies pour adultes se sont multipliées dans de nombreuses villes européennes et américaines[10]. Ces commerces, et derrière eux toute une industrie de vente par correspondance, ont assuré le stockage et la diffusion de très grandes quantités d'articles pornographiques représentant tout l'éventail de gravité. Un certain nombre d'acteurs clés dans le monde se sont immédiatement positionnés sur ce marché pour répondre à la demande de pornographie. Les entrepreneurs ont saisi la balle au bond et un impor-

[10] O'Donnell et Milner, (2007), *Child Pornography, Crime computers and society,* Willan.

tant réseau d'approvisionnement a très rapidement été mis sur pied.

Certains articles pornographiques achetés, vendus et commercialisés contenaient des images d'enfants exploités sexuellement. Les lois promulguées en 1977 aux Etats-Unis contre la diffusion du matériel pédopornographique ont rapidement gagné l'Europe et ont eu pour effet de réduire la production du matériel jusqu'à la rendre illégale. En 1986, les différents circuits d'approvisionnement étaient quasiment tous fermés, ouvrant la possibilité d'une éradication totale du commerce de pornographie enfantine[11].

Qui persistait à vouloir accéder au matériel pédopornographique devait, à cette époque, compte tenu des difficultés rencontrées, accepter de prendre des risques considérables et s'acquitter de coûts particulièrement élevés. L'avènement de l'Internet a ensuite complètement modifié la donne. Le Dr Alvin Cooper cite la «règle des 3 A» applicable à la cybersexualité et facilement transposable à la façon dont l'Internet a révolutionné la possession et la distribution du matériel pédopornographique:

- Accessibilité (l'Internet rend le matériel pédopornographique disponible 24 heures sur 24, 7 jours sur 7 et 365 jours par an);
- Abordabilité (la majorité des articles pédopornographiques sont gratuits et disponibles pour échange ou téléchargement simple);
- Anonymat (les utilisateurs sont convaincus que leurs communications sur l'Internet sont privées et cachées).

Le nouveau contexte a dès lors encouragé les internautes, en l'absence de répercussions visibles, à rechercher et à utiliser du matériel pédopornographique. Qui plus est, le caractère gratuit et disponible du matériel leur laissait à penser que ce dernier était inoffensif.

En 1997, Sir William Utting, éminent expert des services sociaux infantiles, a décrit le commerce du matériel pédopornographique comme une «industrie artisanale»[12]. Ce fut bien la seule fois dans l'histoire où il fut possible de le décrire par ces mots, car il s'agit aujourd'hui d'une véritable industrie mondiale qui ne semble épargner aucun pays.

Il est particulièrement difficile d'évaluer avec précision la taille et la forme d'une activité majoritairement clandestine et souvent illégale. Des estimations en tout genre ont été réalisées à différents endroits pour évaluer le nombre de sites web impliqués[13], le nombre d'enfants exploités aux fins de la production du matériel pornographique[14] et la valeur monétaire globale du marché des images à caractère sexuel. Il est impossible de nier le fait, pour qui connaît le terrain, qu'un très grand nombre d'acteurs est impliqué dans les activités de consultation et de distribution du matériel pédopornographique et qu'il existe une implication du crime organisé[15] dans la distribution commerciale du matériel. Tout comme il est impossible de douter que le nombre d'images illicites actuellement en circulation sur la Toile se monte à plusieurs millions et que les enfants exploi-

[11] Jenkins, P, *Beyond Tolerance*, 2001, New York University Press.

[12] UK, HMSO, 1997.

[13] Dans son rapport annuel 2007, le FMI annonçait que moins de 3000 sites web en langue anglaise étaient responsables de la grande majorité des images d'enfants abusés diffusées en ligne. Trois ans plus tôt, le *Computer Crime Research Center*, basé aux Etats-Unis, estimait leur nombre à plus de 100 000.

[14] Correspondance avec Interpol. Voir le rapport de Telefono Arcobaleno http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf

[15] Voir détails de l'affaire «Reg Pay». http://www.usdoj.gov/criminal/ceos/Press%20Releases/ICE%20Regpay%20PR_080906.pdf

[16] Correspondance avec Interpol mentionnée ci-avant. Dans son rapport, Telefono Arcobaleno parle de 36 000 enfants, dont «42% ont moins de 7 ans et 77% ont moins de 12 ans.» http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf

tés sur ces images se comptent en dizaines de milliers[16]. Et ce n'est là que la partie visible de l'iceberg.

Les *Usenet Newsgroups* constituent à l'origine le principal canal de distribution du matériel pédopornographique sur l'Internet. Bien que toujours largement utilisés, ils se partagent aujourd'hui le marché avec d'autres technologies Internet, dont le *World Wide Web* qui est vraisemblablement la plus importante, car plus accessible et plus facile à utiliser. Certains pays ayant considérablement entravé la distribution du matériel pédopornographique sur le web, on assiste par ailleurs au déploiement d'autres technologies Internet, telles que le Peer2Peer (P2P) ou programmes d'échange de fichiers. Selon Interpol, le P2P est techniquement facile à contrôler, mais le très grand nombre de personnes impliquées rend ce contrôle particulièrement difficile à mettre en œuvre dans la pratique.

A chaque fois que l'image d'un enfant ayant été abusé s'affiche sur l'Internet ou fait l'objet d'un téléchargement, l'enfant est pour ainsi dire abusé une seconde fois. Il est et restera victime tant que ces images perdureront et circuleront. La réaction des victimes et de leurs familles lorsqu'ils apprennent que des images ont été mises en circulation ou publiées sur le net en est le meilleur exemple[17].

C'est pourquoi il est communément admis, après la découverte d'une image ou d'un site web montrant des enfants exploités, que la première étape consiste à supprimer l'image au plus vite, à démonter le site ou à le rendre inaccessible. Un système de hotlines nationales a été développé à cet effet. Des hotlines sont aujourd'hui opérationnelles dans plus de 30 pays différents, et leur nombre ne cesse d'augmenter[18]. Leur croissance est particulièrement souhaitable dans le cadre de la campagne mondiale visant à démanteler le trafic de matériel pédopornographique en ligne.

Il est également une autre raison pour laquelle nous devons immédiatement supprimer toute image illégale trouvée sur l'Internet ou en bloquer l'accès, car plus ces images restent longtemps en circulation, plus elles sont susceptibles d'être trouvées et éventuellement téléchargées par de nouvelles personnes. Et il y a lieu de penser que les personnes qui téléchargent et rassemblent du matériel pornographique sont plus enclines à contacter des enfants dans le monde réel en vue de commettre des délits ou des abus de pornographie enfantine (*From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children. Kim, C (2004)*).

Les autorités chargées de l'application de la loi s'efforcent actuellement d'identifier la victime à partir du matériel pédopornographique diffusé en ligne. Des procédures et des systèmes sont ainsi mis en place au niveau national, et le matériel saisi lors des investigations ou parvenu aux enquêteurs par une autre voie est analysé dans le but de retrouver la victime et, partant, l'auteur de l'abus. Le matériel inconnu jusque-là, dont on ne peut définir la provenance locale, est placé entre les mains d'un réseau international d'enquêteurs et de spécialistes nationaux du matériel pédopornographique. Ce réseau, développé à partir de la base de données internationale sur l'exploitation sexuelle des enfants (ICSE) d'INTERPOL, est coordonné au niveau de la Sous-direction Trafic d'êtres humains d'INTERPOL avec le Groupe de spécialistes d'INTERPOL sur les crimes contre les enfants.

Le but de cette base de données consiste à stocker en un même endroit tout le matériel pédopornographique existant sur l'Internet, tombé aux mains des organes d'application de la loi. Ce matériel est examiné par le réseau international d'experts et, si les conditions le permettent, renvoyé au pays d'origine pour enquêter sur l'identité de l'enfant victime d'abus. Dans le cas contraire, le matériel est archivé dans la base de données avec mention du lieu où il a été trouvé, par qui et quand.

[17] *Child Molesters: a behavioral Analysis*, Kenneth V. Lanning, 2001.

[18] Voir www.inhope.org

De puissants outils de recherche peuvent déterminer si des images ont déjà été rencontrées et bien souvent, des images trouvées dans un pays contiennent des indices permettant d'identifier un cas d'abus dans un autre pays. L'auteur de l'abus apparait parfois sur les images et peut être ainsi appréhendé.

INTERPOL et l'Initiative COP encouragent les meilleures pratiques en matière de lutte contre la pornographie enfantine par la création d'une ressource nationale assurant la gestion centralisée du matériel saisi à l'intérieur des frontières, en vue de créer une base de données nationale et de contribuer par ce biais aux efforts déployés en niveau international.

Cette démarche simplifie le travail des enquêteurs, évite la duplication des efforts au niveau international et, en bout de course, permet l'identification des victimes et l'arrestation des agresseurs.

Harmonisation des lois

L'adoption par les pays d'une législation appropriée pour lutter contre l'usage détourné des technologies de l'information et de la communication (TIC) à des fins criminelles ou autres est une condition essentielle à la promotion de la cybersécurité dans le monde. Les menaces pouvant provenir de n'importe où, les défis à relever ne connaissent pas de frontière et appellent une coopération internationale, une assistance en matière d'enquête ainsi que des dispositions communes de fond et de procédure. Les pays doivent donc impérativement harmoniser leurs cadres législatifs pour combattre le cybercrime, protéger les enfants en ligne et faciliter la coopération internationale.

Le développement de législations nationales appropriées, la mise en place d'un cadre juridique contre le cybercrime et l'harmonisation des lois au niveau international sont autant d'étapes vers le succès des stratégies nationales dédiées à la protection des enfants dans le cyberespace. Il convient, avant toutes choses, d'adopter les dispositions pénales de fond nécessaires pour condamner certains actes, tels que la fraude informatique, l'accès illicite, l'atteinte à l'intégrité des données, les violations de droits d'auteur et la détention de matériel pédopornographique. De telles dispositions existent dans le code pénal pour des actes similaires commis dans le monde réel mais ne sont pas pour autant applicables aux actes commis dans le monde virtuel. La législation nationale en vigueur doit par conséquent être passée au crible pour que soient repérés les éventuels écarts. L'étape suivante consiste à identifier et à définir les termes et les documents législatifs dont les pays pourraient avoir besoin pour édicter des règles de procédure et des lois harmonisées contre le cybercrime. De tels outils peuvent également servir à l'élaboration d'un cadre juridique sur la cybersécurité et des lois correspondantes. L'UIT œuvre en ce sens avec les Etats Membres et les différents intervenants et contribue grandement à promouvoir l'harmonisation des lois contre le cybercrime au niveau mondial.

Le Centre international pour les enfants disparus et exploités (ICMEC, *International Centre for Missing & Exploited Children*) a publié son rapport intitulé «Pornographie enfantine: examen de la législation type à l'échelle mondiale» en avril 2006. L'objectif premier du rapport, qui en est aujourd'hui à sa cinquième édition, visait à mieux comprendre la législation existante en matière de pornographie enfantine et à évaluer l'état actuel de ce problème dans les ordres du jour politiques nationaux. L'étude a porté sur un certain nombre d'éléments, dont la législation portant spécifiquement sur la pornographie enfantine, la législation fournissant une définition de la pornographie enfantine, les lois condamnant la possession sans tenir compte de l'intention de distribution, les lois criminalisant les délits assistés par ordinateur et le signalement par les FAI.

Une copie des résultats détaillés de l'ICMEC est fournie à l'Appendice 4. Il apparaît clairement, à la lecture du rapport, que les approches législatives adoptées par les différents pays présentent d'importantes et considérables disparités. La communauté internationale doit donc trouver un moyen d'apporter une plus grande cohérence dans la façon de traiter ce problème.

Un autre objectif du rapport de l'ICMEC sur la législation type consiste à définir des secteurs dans lesquels une législation est requise pour couvrir au niveau international les différents aspects liés au matériel pédopornographique et aux crimes connexes. A l'instar d'autres types de cybercrimes, la possession, la production et la distribution du matériel pédopornographique ne respectent souvent pas les frontières et rendent nécessaire l'adoption de lois nationales comparables ou équivalentes sur le plan légal – c'est ce que l'on appelle l'harmonisation.

Les auteurs d'abus sexuels sur les enfants, qu'ils utilisent un ordinateur équipé de l'Internet ou qu'ils se rendent directement dans le pays, préfèreront ainsi perpétrer leurs crimes dans des pays dépourvus de législation en la matière ou sans application stricte de la législation existante ou dans des pays situés hors du cadre de la coopération internationale. La lutte contre l'exploitation des enfants, au niveau international, passe par la conformité aux normes légales internationales et l'adoption de lois nationales correspondantes.

De nombreux pays luttent contre l'exploitation des enfants en général, parce qu'il est question de travail illégal ou d'abus en tout genre, ou bannissent tout simplement la pornographie; mais ces mesures ne sont pas suffisantes dans le sens où elles n'englobent pas tous les aspects du droit pénal liés aux différentes formes d'exploitation sexuelle des enfants et aux différentes images d'abus pédosexuels. Pour obtenir une réelle efficacité, les pays doivent adopter une législation spécifique qui condamne le matériel pédopornographique de même que l'utilisation de l'Internet et des technologies à des fins d'obtention de ce matériel. Les criminels tireront autrement avantage des failles existantes dans la législation.

La législation devra également contenir certaines dispositions en faveur d'une plus grande implication des ressources en vue de faire appliquer ces lois spécifiques et de former les responsables de la juridiction, des poursuites et de l'application de la loi, qui doivent savoir comment les criminels utilisent la technologie.

Les principaux points et conseils à observer lors de l'adoption d'une législation sont les suivants:

- définir le terme «enfant» de manière claire et précise, conformément à la Convention des Nations Unies sur les droits de l'enfant;
- définir le «matériel pédopornographique» en veillant à ce que la définition englobe la terminologie spécifique aux ordinateurs et à Internet;
- inscrire de nouvelles infractions dans le code pénal liées à la possession, à la production et à la distribution de matériel pédopornographique, à l'inclusion de pseudo-images, au téléchargement d'images ou à la visualisation d'images de manière délibérée sur l'Internet;
- mettre en place des sanctions pénales pour les parents ou les tuteurs légaux qui autorisent ou encouragent leur enfant à participer à la pornographie enfantine;
- instaurer des sanctions pour ceux qui orientent d'autres personnes vers la pornographie enfantine;
- qualifier d'infractions pénales les tentatives de délits impliquant du matériel pédopornographique;
- définir la responsabilité pénale des enfants participant au matériel pédopornographique. La responsabilité pénale doit concerner l'agresseur adulte et non l'enfant victime;

- majorer les sanctions pour les récidivistes, les membres du crime organisé et en présence d'autres facteurs aggravants pris en considération lors de la détermination de la sentence.

La définition du matériel pédopornographique doit comporter, au minimum, une représentation visuelle ou une description d'un enfant participant à un acte ou à un jeu sexuel, réel ou simulé, ou mis en scène sur des pseudo-images du même type; elle doit également tenir compte de la manière dont l'utilisation de la technologie (ordinateurs, Internet, téléphones cellulaires, PDA, consoles de jeux, caméras vidéo et DVD) facilite la diffusion du matériel pédopornographique, sachant que ledit matériel et tout article connexe est illicite, indépendamment de la plateforme utilisée.

Formation des autorités policières à l'informatique judiciaire

En plus des dispositions de fond du droit pénal, les organismes d'application de la loi doivent avoir à leur disposition des outils et des instruments d'enquête en matière de cybercriminalité. La réalisation d'enquêtes présente un certain nombre de gageures, compte tenu du fait que les criminels peuvent agir de n'importe où dans le monde et prennent des mesures pour masquer leur identité. Les outils et les instruments requis dans le cadre des enquêtes sur les cybercrimes peuvent être très différents de ceux utilisés pour les crimes ordinaires.

Les auteurs de crimes pédosexuels utilisent aujourd'hui systématiquement l'Internet, les ordinateurs, les téléphones cellulaires, les PDA et autres appareils numériques. La technologie sur laquelle reposent ces équipements est de plus en plus complexe et évolue à un rythme toujours plus rapide. Pour pouvoir récupérer et conserver les preuves laissées par les criminels, les autorités de police doivent bénéficier d'une formation et d'une expertise technique leur permettant de traiter les preuves conformément aux exigences judiciaires aux niveaux national et international. Une formation doit par conséquent être dispensée à l'intention des responsables de l'application de la loi, de la juridiction et des poursuites pour les aider à comprendre comment conduire une analyse judiciaire des disques durs et des autres équipements informatiques. Une telle formation se doit d'être constamment actualisée pour suivre les évolutions incessantes de la technologie et fournir une expérience du terrain. De nombreuses suites logicielles offrent les outils qui permettent de réaliser des examens en lecture seule des médias saisis, la formation étant souvent incluse dans le prix d'achat. Mais ces solutions sont souvent trop onéreuses et donc non accessibles aux pays en développement. Des formations peuvent être organisées au sein des services de police et des services de sécurité privés sur la base de financements internes.

Nombre de sociétés du secteur privé disposent de la technologie et de l'expertise nécessaires pour ce type de travail. Des partenariats public/privé pourraient donc s'avérer particulièrement bénéfiques sur le plan de la formation et de l'assistance technique.

Coopération internationale et partage des données

Il importe de développer davantage la coopération internationale et le partage des données.

L'une des tâches essentielles confiée à l'UIT lors du SMSI consiste à établir la confiance et la sécurité dans l'utilisation des TIC. Les chefs d'Etat et de gouvernement et autres dirigeants du monde entier ayant pris part

au SMSI, ainsi que les Etats Membres de l'UIT, ont chargé l'UIT de prendre des mesures concrètes visant à limiter les répercussions des cybermenaces et de l'insécurité liée à la société de l'information.

Le SMSI estime que la grande orientation C5 regroupe un grand nombre de thématiques et d'acteurs. Comme indiqué dans le paragraphe 110 de l'Agenda de Tunis, «*la coordination des activités de mise en œuvre multi-parties prenantes contribuerait à éviter les doubles emplois. Cette coordination devrait comprendre notamment l'échange d'informations, la création de savoirs, l'échange des meilleures pratiques et l'aide en faveur de l'établissement de partenariats multi-parties prenantes et de partenariats public/privé*».

INTERPOL[19], avec un réseau de 187 pays membres, a pour mission de faciliter les échanges d'informations entre les services de police. Ce réseau permet l'échange instantané d'informations entre les pays et, grâce au déploiement du système i24/7, directement aux unités spécialisées.

Lorsque la communication d'informations et de preuves pénètre la sphère judiciaire, les règles de la coopération sont régies par le cadre juridique ainsi que par les dispositions des conventions multilatérales et des traités bilatéraux d'entraide juridique, qui ne suivent pas toujours l'évolution rapide de l'Internet.

Si le pays n'est pas doté d'une loi nationale imposant la coopération, une assistance ne sera pas fournie ou ne le sera que de manière très restrictive, indépendamment des accords convenus. La partie qui fournit les informations peut fixer les conditions régissant l'utilisation de ces informations et exiger la confidentialité.

Il est nécessaire d'adopter une approche coopérative pour parvenir à un consensus mondial sur ces éléments communs qui doivent faire partie du cadre juridique destiné à protéger les enfants dans le cyberespace. Face à une cybercriminalité et, en particulier, à l'exploitation des enfants sans frontières, les organismes chargés de l'application de la loi doivent impérativement coopérer au niveau international pour apporter une solution mondiale au problème.

[19] INTERPOL coordonne également les activités du groupe spécialisé INTERPOL sur la criminalité contre l'enfance, qui se réunit en session une fois par an. Le groupe de travail se subdivise en cinq sous-groupes dont les membres se rencontrent virtuellement tout au long de l'année pour collaborer sur des projets. Ces secteurs concernés sont les suivants: la cybercriminalité contre les enfants, les pédocriminels, le trafic d'enfants, les crimes sérieux et violents commis contre les enfants et l'identification des victimes en vue de faciliter la coopération internationale au quotidien avec la base de données mondiale des enfants ayant subi des abus sexuels.

Obligation de signalement

Toute personne qui découvre du matériel pédopornographique est normalement tenue de signaler son existence aux autorités de police et/ou à une hotline nationale[20]. On distingue trois catégories de personnes et d'organisations ayant particulièrement intérêt à révéler la présence suspectée de matériel pédopornographique, que ce soit directement à la police ou à une autre entité désignée telle qu'une hotline:

1. Les personnes qui, dans le cadre de leur activité professionnelle, sont en contact avec des enfants et ont une obligation de vigilance envers ces enfants (professeurs, formateurs, conseillers, prestataires de soins, agents de la force publique, etc.).

2. Les personnes qui, dans le cadre de leur activité professionnelle, ne sont pas nécessairement en contact avec des enfants mais qui peuvent être exposés à du matériel pédopornographique dans certaines situations (techniciens en informatique, développeurs de photos, etc.).

3. Les organisations ou sociétés dont les services sont utilisés pour la diffusion du matériel pédopornographique et qui, par conséquent, devraient avoir une responsabilité sociale au niveau de l'entreprise (FAI et autres fournisseurs de services électroniques, sociétés émettrices de cartes de crédit, banques, etc.).

La composition des groupes 1 et 2 va de soi. Elle est moins évidente, en revanche, pour les FAI, les banques et les sociétés émettrices de cartes de crédit dont les services, essentiels à la transmission du matériel pédopornographique, sont «détournés» par les pédocriminels. Ces acteurs peuvent obtenir, de par leur positionnement, des preuves de l'existence de matériel pornographique et sont vivement encouragés à coopérer avec les autorités et à leur fournir tout renseignement sur ledit matériel rencontré.

Il est à noter que certaines sociétés fournissent actuellement une assistance précieuse en la matière. Les FAI et autres fournisseurs de services électroniques sont plus enclins que d'autres à tomber sur du matériel pédopornographique au travers des fichiers, URL, noms de domaines et images qu'ils traitent et doivent signaler leur existence aux autorités dans les plus brefs délais. Qui plus est, le partage des URL, des noms de domaine et des adresses IP facilite le trafic des bretelles d'accès vers les principaux sites à caractère pédosexuel. Les fournisseurs sont par conséquent tenus de scanner activement leurs réseaux à la recherche de matériel pédopornographique et de rendre compte aux autorités compétentes chargées de l'application de la loi.

Eu égard au rôle joué par l'Internet et à l'utilisation qui en est faite par les criminels, il apparaît aujourd'hui essentiel de coopérer avec les sociétés basées sur l'Internet. La législation devrait par ailleurs offrir une protection aux FAI, aux fournisseurs de services électroniques et aux autres entités privées qui rapportent l'existence de matériel pédopornographique et devrait fournir des conseils en vue du traitement et de la transmission sécurisés des images.

Une procédure d'avis et de retrait («*notice and takedown regime*») doit permettre aux FAI, aux fournisseurs de services électroniques, aux gestionnaires des noms de domaine et aux fournisseurs de services d'hébergement de fermer un site incriminé ou d'annuler un compte de messagerie sur demande. Dans la majorité des cas, l'usage illicite constaté ne respecte pas les conditions d'utilisation convenues entre le client et le FAI ou le fournisseur de services électroniques, ce qui donne à la société le droit incontestable

[20] Les hotlines nationales soumettent des rapports aux autorités chargées de l'application de la loi. Ces dernières analysent les rapports en question pour effectuer des recoupements au niveau local ou transmettent les informations à la base de données mondiale sur les enfants victimes d'abus sexuels, pour analyse.

d'adopter les mesures jugées appropriées. Si possible, ces actions seront coordonnées en étroite collaboration avec les autorités de police, de façon à mieux prévenir les abus pédosexuels et à augmenter les chances d'arrestation des criminels.

La vente en ligne de matériel pédopornographique est aujourd'hui activité mondiale lucrative qui utilise les services bancaires, les virements électroniques et les cartes de crédit pour en faciliter la vente, la transmission et la distribution. Les responsables de l'industrie financière qui pourraient être amenés à avoir connaissance de certains éléments d'information en la matière sont tenus de rendre compte aux autorités compétentes. Les sites concernés imposent souvent un système de paiement à la consultation («*pay per view*») ou des droits d'inscription et acceptent de fait les paiements par carte de crédit ou par virement.

De façon générale, l'industrie des services financiers devrait coopérer à l'instar du modèle fourni par la *Financial Coalition Against Child Pornography* (FCACP)[21], conjointement mis en place par le Centre international pour les enfants disparus et exploités (ICMEC) et son organisation sœur, le Centre national pour les enfants disparus et exploités(NCMEC). La coalition financière fournit des outils de coopération efficace au service de l'industrie des services financiers, de l'industrie des services Internet, des organismes d'application de la loi et des organisations non gouvernementales. Elle a remporté un vif succès en empêchant les fournisseurs de matériel pédopornographique d'utiliser le système financier international. Grâce à une collaboration étroite, ses membres sont parvenus non seulement à dénoncer certaines transactions et comptes suspects, mais également à suivre des activités de compte et des mouvements de trésorerie qui les ont menés jusqu'aux personnes et organisations responsables de la commercialisation du matériel pédopornographique. Une version européenne de cette coalition a été lancée en 2009.

Réduire la disponibilité des images d'abus pédosexuels

La prolifération du matériel pédopornographique sur l'Internet suscite de vives réactions. Dans le monde entier, les autorités chargées de l'application de la loi, les FAI, les fournisseurs de services électroniques et les organisations non gouvernementales jouent la carte de la main tendue pour combattre ces contenus. Les autorités de police ne peuvent s'en sortir seules et de nombreux efforts restent à accomplir pour entraver et réduire la propagation de la pornographie enfantine. De nombreux pays ont ainsi commencé à explorer de nouvelles voies, lesquelles viennent compléter les approches traditionnelles des services police.

Une approche adoptée dans plusieurs pays consiste à encourager les FAI et autres fournisseurs de services électroniques à réduire la disponibilité des pages web notoirement utilisées pour accueillir du matériel pédopornographique et à bloquer l'accès aux *Usenet Newsgroups* qui contiennent régulièrement ce type de contenu ou affichent leur disponibilité.

Dans le cadre de cette démarche, une «liste» des *Usenet Newsgroups* et des pages web actives contenant ou faisant la publicité de pornographie enfantine est remise aux FAI et fournisseurs de services électroniques. Cette liste est établie et fournie par les service de police ou, dans certains cas, directement par les hotlines nationales, et doit être clairement articulée à sa base. Elle doit écarter toute suspicion d'influence du gouvernement, des forces de police ou d'autres entités sur sa composition, comme l'inclusion de *Newsgroups* ou de sites web ne renfermant pas de matériel pédopornographique mais contenant des articles dont la publication n'est pas souhaitée pour d'autres raisons.

La production et la diffusion de la liste aux FAI et fournisseurs de services électroniques nécessitent l'amorce d'un dialogue préalable avec les services de police,

[21] FCACP: http://www.icmec.org/missingkids/servlet/PageServlet?LanguagePays=en_X1&PageId=3064.

lesquels ont besoin de temps pour obtenir, examiner, documenter le contenu et, le cas échéant, lancer une enquête. L'absence de prise de contact peut bloquer ou retarder une enquête en cours. Les diffuseurs de matériel pédopornographique ne pourraient pas être arrêtés, ni traduits en justice sans la participation et les enquêtes de la police.

Il importe régulièrement de tester, de mettre à jour et de vérifier la liste des *Usenet Newsgroups* et des sites connus pour garantir l'exactitude des données. Une procédure de tests multiples évitant les chevauchements assurera la confiance du public dans les opérations. Il faut également veiller à la transparence des règles relatives aux critères de la liste. Certains pays procèdent à une évaluation autonome des performances et des opérations. Enfin, il devrait exister un mécanisme permettant d'exclure tout ajout sur la liste. Les seuls sites y figurant sont ceux autorisant la publication ou l'affiche de contenus reconnus comme illicites par les lois nationales du pays concerné. Lorsqu'un site est bloqué, une page STOP s'affiche. Cette page STOP fournit d'une part à l'utilisateur les raisons du blocage (illégalité du contenu) et joue d'autre part un rôle préventif en avertissant l'utilisateur/le consommateur de la nature illicite du matériel ainsi que de la présence en ligne des autorités d'application de la loi.

Le fait de bloquer l'accès aux sites web et aux *Usenet Newsgroups* contenant du matériel pédopornographique peut contribuer de façon importante à entraver et à réduire les volumes qui circulent et qui sont diffusés sur l'Internet. Cela ne représente pourtant qu'une partie de la solution qui ne peut se résumer à cette seule approche. L'objectif consiste à soutenir les efforts des autorités chargées de l'application de la loi et à réduire la disponibilité du matériel pédopornographique en ligne. Les individus ayant un intérêt sexuel pour les enfants ainsi que suffisamment de détermination et de savoir-faire technique sauront toujours localiser ces contenus. Mais le web, doté d'une interface ultraconviviale, est devenu l'une des applications Internet les plus populaires et les plus utilisées. Il apparaît donc essentiel de développer des approches spécifiques visant à maîtriser l'outil Internet tout en continuant d'évaluer de nouvelles méthodes pour contrecarrer la distribution sur les autres plateformes.

Ne perdons pas de vue l'idée de lancer une campagne média de sensibilisation, conjointement organisée par le gouvernement et l'industrie, à l'intention des consommateurs de matériel pédopornographique. Il importe de rappeler aux utilisateurs/consommateurs que le matériel pédopornographique peut causer un réel préjudice aux enfants dans la vraie vie et que la création, la possession et la distribution de ce matériel constituent un acte illégal dans de nombreux pays.


«Les enfants et les adolescents sont souvent particulièrement vulnérables en ligne»

4.

Principaux risques auxquels les enfants sont exposés en ligne

Les adultes comme les enfants sont exposés dans le cyberespace à toute une série de risques et de dangers, mais les enfants et les adolescents sont souvent particulièrement vulnérables. Les enfants notamment, qui sont en phase de développement et d'apprentissage, ne sont pas toujours à même d'identifier, d'évaluer et de gérer les risques susceptibles de se présenter à eux. La Convention des Nations Unies relative aux droits de l'enfant[22] souligne le caractère vulnérable des enfants et la nécessité de les protéger contre toute forme d'exploitation.

Un certain nombre de questions relatives à l'utilisation de l'Internet par les enfants et les adolescents ne cessent de requérir l'attention des parents et des enfants ainsi que des gouvernements, des politiques et des organes de décision. Ces préoccupations portent notamment sur les points suivants:

Contenus

- Les enfants et les adolescents peuvent être exposés à des contenus illicites, tels que du matériel pédopornographique.
- Les enfants et les adolescents peuvent être exposés à des contenus licites mais inadaptés à leur âge, tels que des images très violentes.

[22] http://www.unhchr.ch/html/menu3/b/k2crc.htm

Contacts

- Les enfants et les adolescents peuvent être exposés à des prédateurs sexuels, que ces derniers soient adultes ou mineurs[23].
- Les enfants peuvent être exposés à des communautés en ligne aux contenus préjudiciables, telles que des sites qui encouragent l'anorexie, l'autodestruction ou le suicide, ou à des sources d'influence politique qui prônent la violence, la haine et l'extrémisme.

Comportement

- L'Internet facilite et encourage les interactions sexuelles à risque entre les enfants, en les incitant à prendre et à diffuser des clichés d'eux-mêmes ou d'autres (*sexting*), une pratique non seulement dommageable mais également illicite. Le développement normal de la vie sexuelle et les expérimentations en ligne peuvent parfois donner lieu, par inadvertance, à la production et à la diffusion de matériels à caractère sexuel qui exposent l'enfant ou ses camarades à des sanctions juridiques jusqu'à impliquer parfois le système de justice pénale.
- Les enfants peuvent être incités à rendre publiques des informations personnelles ou à poster des images, des vidéos ou du texte pouvant compromettre leur propre sécurité ou proscrire certains choix de carrière pour l'avenir.
- L'Internet peut exposer les enfants et les adolescents à des manœuvres d'intimidation et permettre, voire favoriser, un environnement au sein duquel les enfants et les adolescents seraient eux-mêmes incités à user de telles manœuvres.

Commerce

- Les enfants et les adolescents peuvent posséder et acquérir des biens et des services inappropriés pour leur âge, notamment des biens et des services qu'ils ne pourraient pas acheter en personne dans un magasin.
- Les enfants et les adolescents peuvent être exposés à des arnaques, à des vols d'identité, à des fraudes et autres menaces similaires de nature économique ou en violation des lois sur la protection des données et de la sphère privée.

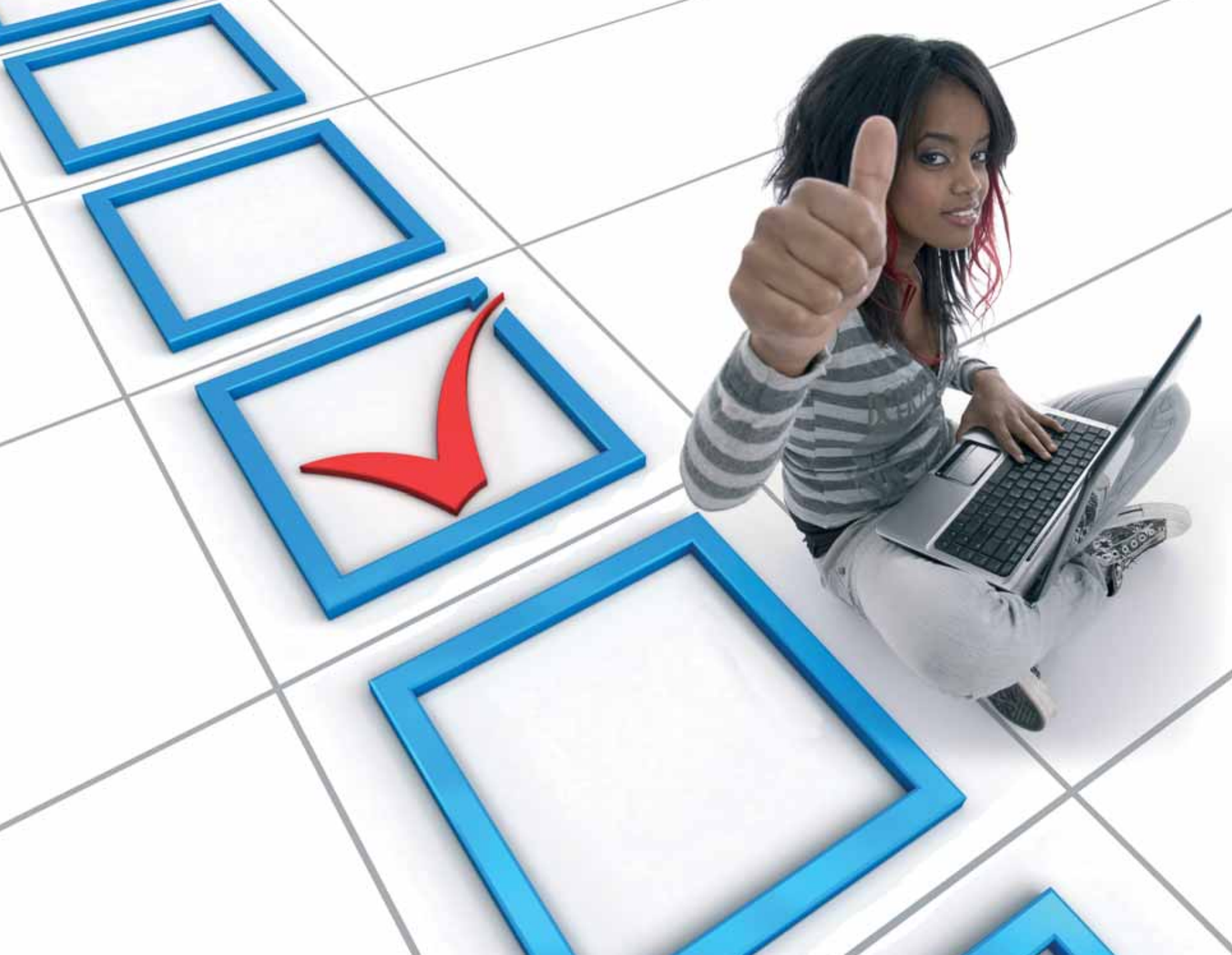
Utilisation excessive

- L'Internet semble avoir révélé chez certains enfants et adolescents des comportements obsessionnels et une utilisation excessive, pouvant avoir des effets délétères sur la santé, sur la vie sociale, voire les deux. Le jeu sur l'Internet est souvent déclencheur de ce comportement considéré dans certains pays comme une forme de dépendance.

Aspects de société

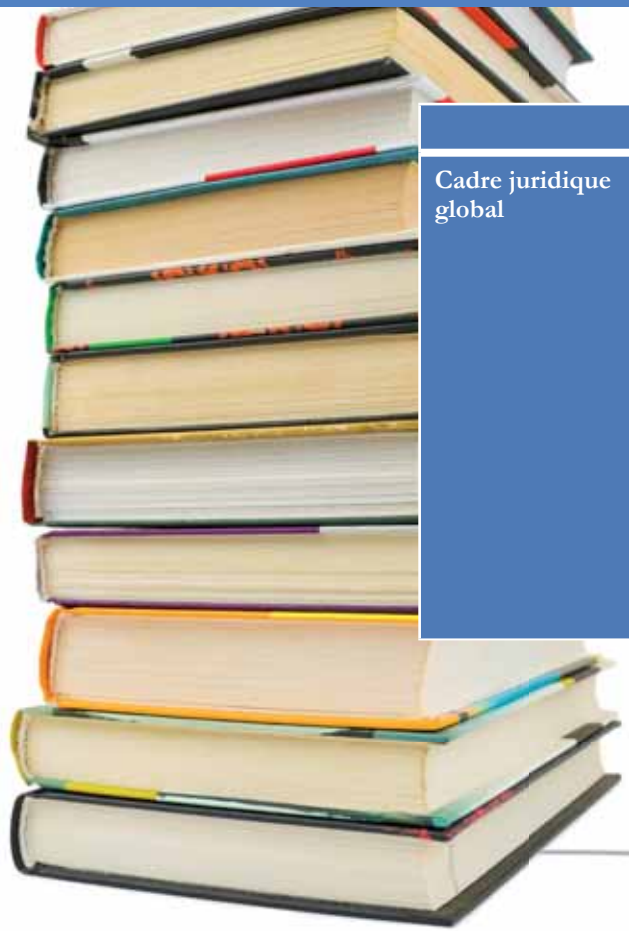
- L'Internet a créé un nouveau fossé numérique parmi les enfants et les adolescents, entre ceux qui y ont facilement et rapidement accès – chez eux, à l'école ou dans un autre lieu – et les autres, ou entre ceux qui sont des utilisateurs confiants et avertis et les autres. Ce fossé menace de déséquilibrer encore la balance entre avantages et inconvénients ou de provoquer de nouvelles scissions.
- L'Internet est de nature à souligner et exacerber vulnérabilités existantes chez certains enfants et adolescents, qui viennent ainsi se rajouter aux difficultés rencontrées dans la vie réelle.

[23] Voir l'Appendice 1 pour plus de détails sur ce thème,



5. La gestion des risques

Liste de contrôle nationale



	#	Liste de contrôle nationale
Cadre juridique global	1.	Il est généralement nécessaire de mettre en place un ensemble de lois qui établissent clairement que tout crime commis contre un enfant dans le monde réel peut également, *mutatis mutandis*, être commis sur l'Internet ou par le truchement de tout autre réseau électronique. Il peut être également nécessaire de promulguer de nouvelles lois ou d'adapter les lois existantes afin d'interdire certains types de comportement qui ne peuvent exister que sur l'Internet, par exemple le fait d'inciter les enfants à distance à participer ou à assister à des jeux sexuels ou encore de les «préparer» à une rencontre dans le monde réel à des fins sexuelles. Parallèlement, il conviendra d'instaurer un cadre juridique qui proscrive l'utilisation détournée des ordinateurs à des fins criminelles, qui empêche le piratage informatique et toute autre utilisation malveillante ou non-consensuelle du code informatique et qui stipule que l'Internet est un lieu dans lequel des crimes peuvent être perpétrés.

	#	Liste de contrôle nationale
Nécessité de mener une action nationale pour la protection des enfants en ligne	2.	Plusieurs gouvernements nationaux ont jugé utile de rassembler les principaux acteurs et l'ensemble des parties prenantes afin d'élaborer et de mettre en œuvre une initiative nationale visant à faire de l'Internet un lieu plus sûr pour les enfants et les adolescents et afin d'accroître la sensibilisation du public aux problèmes rencontrés et à la manière de les aborder sous un angle pratique. Il est important de noter, dans le cadre de cette stratégie, que toutes sortes d'équipements permettent aujourd'hui d'accéder à l'Internet. Les ordinateurs ne représentent qu'un moyen parmi d'autres de se connecter au réseau mondial. Les téléphones mobiles, les consoles de jeux et les PDA, pour ne citer qu'eux, sont de plus en plus utilisés. Il convient par conséquent d'impliquer les fournisseurs d'accès fixe et sans fil. Dans de nombreux pays, le réseau des bibliothèques municipales, les télécentres et les cafés Internet offrent plusieurs bornes d'accès à l'Internet, à destination notamment des enfants et des adolescents. Certains pays ont estimé qu'il était avantageux d'établir un modèle autoréglementé ou coréglementé régissant l'élaboration des politiques dans le secteur. De tels modèles ont ainsi permis la publication de codes de bonnes pratiques qui ont fourni des recommandations à l'industrie Internet sur les meilleures mesures à appliquer pour assurer la sécurité des enfants et des adolescents en ligne. La démarche a également été adoptée au niveau régional: des codes européens sur les sites de réseautage social et sur les réseaux de téléphonie mobile ont ainsi été publiés au sein de l'Union européenne en relation avec la fourniture de contenus et de services à destination des enfants et des adolescents via ces réseaux. L'autorégulation et la corégulation sont deux outils très efficaces pour attirer et maintenir l'implication de toutes les parties prenantes et s'avèrent particulièrement utiles également pour formuler et mettre en œuvre rapidement des stratégies en réponse aux évolutions technologiques. Les écoles et le système éducatif jouent généralement un rôle prépondérant dans le déploiement de ce type de stratégie nationale, mais la stratégie doit aller plus loin.

	#	Liste de contrôle nationale
Nécessité de mener une action nationale pour la protection des enfants en ligne		Il convient par ailleurs de lister les moyens pouvant être proposés par les médias de masse pour promouvoir les campagnes et les messages de sensibilisation.
Nécessité de développer des ressources locales conformes aux lois nationales et aux normes culturelles locales	3.	Les grandes sociétés Internet, pour la plupart, diffusent sur leurs sites un grand nombre d'informations relatives à l'utilisation en ligne par les enfants et les adolescents. Malheureusement, ce matériel n'est trop souvent disponible qu'en langue anglaise ou dans un nombre très restreint de langues. Ce matériel doit impérativement être produit localement, en conformité avec les lois nationales et avec les normes culturelles locales, pour toutes les campagnes liées à la sécurité sur Internet et pour toute la documentation de formation.
Nécessité d'éduquer le public et de mener des activités de sensibilisation	4.	Les parents et les tuteurs de même que les professionnels tels que les enseignants ont un rôle crucial à jouer pour permettre aux enfants et aux adolescents de naviguer sur l'Internet en toute sécurité. Des programmes d'éducation et de sensibilisation doivent être mis en place pour aborder les problématiques soulevées et concevoir des stratégies adaptées. Il ne faut pas perdre de vue, lors de l'élaboration du matériel pédagogique, que les nombreuses personnes non familières avec la technologie éprouveront des difficultés à l'utiliser. Aussi, les éléments relatifs à la sécurité devront-ils être communiqués par écrit ou par le biais d'un autre média avec lequel les nouveaux venus seront plus familiers (par exemple, la vidéo). Comme dans toute campagne d'éducation et de sensibilisation, il importe de trouver le bon ton, d'éviter les messages suscitant la peur et de mettre en avant les nombreuses solutions positives et attrayantes offertes par la nouvelle technologie. L'Internet offre aux enfants et aux adolescents d'incroyables possibilités de découvrir de nouveaux univers, mais les programmes d'éducation et de sensibilisation doivent impérativement donner la priorité à l'apprentissage d'un comportement en ligne à la fois positif et responsable.

	#	Liste de contrôle nationale
Nécessité de signaler les comportements prédateurs en ligne, y compris les actes d'intimidation	5.	Il est nécessaire d'encourager et de promouvoir, sur l'Internet ou par le biais d'un autre média, la démarche qui consiste à dénoncer par exemple à la hotline nationale les abus sur les services en ligne ainsi que les cybercomportements jugés répréhensibles ou illicites. Les liens permettant de signaler les cas d'abus doivent être placés en évidence sur tout site web permettant l'affichage de contenu généré par l'utilisateur. Les personnes qui se sentent menacées de quelque manière que ce soit ou les personnes qui ont été témoins d'une activité inquiétante sur l'Internet doivent également pouvoir rendre compte dans les plus brefs délais aux autorités policières, lesquelles doivent être formées et préparées pour apporter une réponse pertinente. Le *Virtual Global Taskforce* est un organisme d'application de la loi qui fournit une assistance, 24 heures sur 24 et 7 jours sur 7, permettant de recueillir les signalements de comportements ou de contenus illicites en provenance des Etats-Unis, du Canada, de l'Australie et de l'Italie. D'autres pays devraient prochainement adhérer à l'initiative. Des renseignements complémentaires peuvent être obtenus à l'adresse www.virtualglobaltaskforce.com
Nécessité d'utiliser des outils techniques pour assurer la sécurité des enfants	6.	De nombreux programmes logiciels peuvent supprimer les contenus non sollicités ou bloquer les contacts non souhaités. Certains de ces programmes de filtrage ou de contrôle parental sont gratuits, car faisant partie du système d'exploitation de l'ordinateur, ou inclus dans un package fourni par le FAI ou un autre fournisseur de services électroniques. Les fabricants de consoles de jeux peuvent également proposer de tels outils à partir du moment où leurs consoles sont dotées d'une connexion Internet. Ces programmes ne sont pas sûrs à 100%, mais représentent une aide particulièrement appréciée, en particulier dans les familles comptant de jeunes enfants. Ces outils techniques doivent faire partie d'un dispositif plus large. L'implication des parents et/ou des tuteurs est essentielle. Au fur et à mesure qu'ils grandissent, les enfants réclament plus d'intimité et souhaitent de plus en plus ardemment explorer le monde par eux-mêmes. S'il existe par ailleurs une relation de facturation directe entre le vendeur et le client, les procédures de vérification de l'âge peuvent jouer un rôle plus que significatif auprès des vendeurs de biens et services soumis à une limite d'âge ou auprès des diffuseurs de contenus destinés à un public à partir d'un certain âge pour les aider à atteindre leur public cible. En l'absence d'une relation de facturation directe, l'utilisation des techniques de vérification de l'âge peut être problématique, voire impossible dans de nombreux pays en raison du manque de sources de données fiables.

Lignes directrices à l'intention des décideurs

6. Parties prenantes

En vue de développer une stratégie nationale visant à promouvoir la sécurité des enfants et des adolescents dans le cyberespace, les gouvernements nationaux et les instances de décision doivent pouvoir identifier et impliquer les différentes parties prenantes.

Enfants et adolescents

Les enfants et les adolescents du monde entier font montre d'une très grande capacité d'adaptation en ce qui concerne l'utilisation des nouvelles technologies. A la fois plate-forme de travail, de jeu et de communication, l'Internet est de plus en plus présent dans les écoles.

Les enfants et les adolescents, pour la plupart, n'éprouvent aucune appréhension face au monde de l'Internet et utilisent aisément les différents équipements qui permettent de s'y connecter. Ils savent souvent mieux que leurs parents et que leurs enseignants comment fonctionnent l'ordinateur et l'Internet.

Mais la connaissance n'est pas la sagesse, et le manque d'expérience de la vie en général rend les enfants et les adolescents vulnérables à de nombreux risques. Ils ont un droit à l'assistance et à la protection. Il est important de noter également que tous les enfants et les adolescents n'expérimentent pas l'Internet et les nouvelles technologies de la même manière. Les enfants qui ont des besoins spécifiques en raison d'incapacités physiques ou autres sont, par exemple, plus vulnérables dans le cyberespace et nécessitent une assistance complémentaire.

Des enquêtes ont révélé à maintes reprises qu'il pouvait exister des décalages très importants entre ce

que les adultes pensent et ce que les enfants et les adolescents font réellement dans le cyberespace. C'est pour cette raison notamment qu'il convient de trouver des mécanismes appropriés – quels que soient les arrangements réalisés au niveau national pour développer les politiques sur le thème – permettant de laisser les enfants et les adolescents s'exprimer et de prendre en compte leurs expériences concrètes en matière d'utilisation de la technologie.

Parents, tuteurs et éducateurs

Si de nombreux parents achètent pour le domicile des ordinateurs équipés d'une connexion Internet, c'est en partie pour donner à leurs enfants la meilleure éducation possible et pour les aider à faire leurs devoirs scolaires. Les écoles, quant à elles, ont la responsabilité d'enseigner aux enfants la manière d'utiliser l'outil en toute sécurité quel que soit le lieu de connexion (école, domicile ou autre). Pour remplir cette mission, les enseignants doivent eux-mêmes recevoir une formation professionnelle et disposer de ressources d'enseignement actualisées de premier ordre.

Les parents et les tuteurs sont presque toujours le premier, le dernier et le meilleur rempart pour leurs enfants en matière de défense et d'assistance. Lorsque l'on pénètre la sphère de l'Internet, toutefois, ils peuvent sembler quelque peu perdus. Les écoles ont à nouveau un rôle majeur à jouer pour sensibiliser les parents et les tuteurs aux risques de même qu'aux extraordinaires possibilités engendrées par les nouvelles technologies. Toutefois, les écoles ne doivent pas constituer l'unique moyen d'action sur les parents et les tuteurs. Il importe en effet d'utiliser tout l'éventail des canaux disponibles pour sensibiliser le plus grand nombre possible d'intervenants. Les bibliothèques municipales, les établissements de soins, les centres commerciaux et autres grands centres de commerce de détail offrent des espaces où il est possible de diffuser certaines informations relatives à la sécurité.

Industrie

Les sociétés qui développent ou fournissent des biens et services basés sur les nouvelles technologies sont particulièrement bien positionnées pour aider les autres parties prenantes à comprendre le fonctionnement de ces nouvelles technologies et leur expliquer comment les utiliser de manière sûre et appropriée. Il est donc essentiel d'impliquer ces entreprises pour les inciter à partager leur savoir et leur expertise.

L'industrie a également un devoir d'information vis-à-vis des enfants et des adolescents, de leurs parents ou tuteurs et de la communauté au sens large, sur les questions liées aux activités et à la sécurité en ligne. Les entreprises qui se conforment à cette obligation sont plus en phase avec les besoins et les attentes des différentes parties prenantes, ce qui leur permet d'identifier certains risques sur des produits et services en développement, voire d'apporter des corrections sur des produits et services existants.

Dans certains pays, l'Internet est régi par un modèle autoréglementé ou coréglementé. Autrement dit, l'industrie Internet a voix au chapitre dans l'élaboration des politiques gouvernementales et contribue à garantir la validité technique des politiques. La présence d'un tel cadre permet également des ajustements rapides sur le terrain, en réponse aux changements technologiques, sans passer par l'application de procédures d'élaboration parfois fastidieuses et par la promulgation de nouvelles lois. Si le fait d'impliquer l'industrie pour promouvoir une meilleure compréhension des questions liées à la sécurité en ligne revêt un caractère essentiel, il est tout aussi important pour les gouvernements nationaux et les autres membres de la communauté des décideurs de posséder leurs propres sources d'information.

Chercheurs et ONG

Au sein des universités et du monde de la recherche en général, il n'est pas rare de trouver toute une série d'universitaires et de chercheurs qui étudient et connaissent parfaitement bien les aspects et l'impact de l'Internet sur les plans social et technique. Ces acteurs peuvent apporter une contribution précieuse aux gouvernements nationaux et aux décideurs chargés d'élaborer des stratégies fondées sur les faits indéniables et sur la force probante. Ils peuvent également servir de contrepoids intellectuel face aux entreprises high-tech dont les intérêts sont parfois court-termistes et de nature essentiellement commerciale.

De même, la communauté des ONG renferme bien souvent une mine précieuse d'expertises et d'informations pouvant être placées au service des enfants, des adolescents, des parents, des tuteurs et des éducateurs pour promouvoir la sensibilisation aux questions de sécurité en ligne.

Organismes d'application de la loi

Aussi merveilleuse soit-elle, la technologie attire malgré elle les criminels et les comportements antisociaux. Force est de constater que l'Internet a considérablement accru la circulation du matériel pédopornographique. Les prédateurs sexuels utilisent le net pour entrer en contact avec les enfants et les adolescents et les attirer dans leurs filets, en ligne et hors-ligne. Les brimades et autres formes d'intimidation peuvent avoir de graves conséquences sur la vie des enfants et des adolescents, et l'Internet a ouvert de nouvelles portes dans ce domaine.

Il est dès lors essentiel, au vu de ces éléments, d'impliquer pleinement les organismes d'application de la loi dans l'élaboration des stratégies visant à rendre l'Internet plus sûr pour les enfants et les adolescents. Les agents de la force publique ont besoin d'une formation adaptée pour pouvoir mener des enquêtes sur les cybercrimes commis contre les enfants et les adolescents. Ils doivent disposer des compétences techniques nécessaires et accéder aux établissements de défense sociale pour pouvoir extraire et interpréter les données fournis par les ordinateurs et l'Internet.

Les organismes d'application de la loi doivent par ailleurs instaurer des mécanismes clairs permettant aux enfants et aux adolescents de signaler des cas d'abus ainsi qu'à toute autre personne de rendre compte d'incidents ou d'inquiétudes concernant la sécurité en ligne d'un enfant ou d'un adolescent. De nombreux pays ont ainsi mis en place des hotlines pour recueillir plus facilement les signalements de pornographie enfantine ainsi que d'autres mécanismes pour d'autres types de signalement, tels que des cas de brimade et autres formes d'intimidation.

Les forces de police sont les premières à recevoir le matériel pédopornographique saisi à l'intérieur des frontières nationales. Elles lancent une procédure d'enquête pour tenter d'identifier des victimes au niveau local. En cas d'échec, le matériel est transmis à Interpol et enregistré dans la base de données ICSE.

Services sociaux

Les enfants et les adolescents qui ont été maltraités ou abusés en ligne (par exemple, une photo d'eux indécente ou illicite a été diffusée sur le net) ont très souvent besoin d'une assistance et de conseils spécialisés sur le long terme. Les professionnels des services sociaux doivent recevoir une formation adaptée pour être en mesure de dispenser ce type d'aide.

7. Conclusion

L'Internet est devenu un média incontournable qui intègre diverses technologies numériques capables de transformer les économies et d'ouvrir un champ extraordinaire de possibilités d'amélioration de la vie des personnes et d'enrichissement de la société par différents biais.

A l'échelon macro-économique, les avantages apportés par l'Internet doivent être impérativement répartis dans le monde de manière équitable. La problématique de l'élargissement du fossé numérique entre les pays développés et les pays en voie d'industrialisation, qui perpétue ou accentue les désavantages ou déséquilibres existants, a été abordée lors du processus du SMSI. Ce point figure toujours à l'ordre du jour des discussions politiques menées au sein du Forum du SMSI[24], du Forum sur la gouvernance de l'Internet (FGI)[25] et de nombreux forums internationaux consacrés à des thèmes connexes.

Au niveau individuel, l'Internet est un outil excessivement enrichissant et formateur. Les enfants et les adolescents tout particulièrement sont les premiers utilisateurs de l'Internet et des technologies numériques qui lui sont associées. Ces techniques ont révolutionné notre façon de communiquer et ouvert de nouveaux horizons pour jouer, écouter de la musique et se livrer à toutes sortes d'activités culturelles par delà les frontières spatiales et temporelles. Les enfants et les adolescents sont très souvent en première ligne lorsqu'il s'agit d'adopter et de s'adapter aux nouvelles possibilités offertes par l'Internet.

[24] http://www.itu.int/wsis/implementation/2009/forum/geneva/index.html

[25] www.intgovforum.org

Nul ne peut ignorer toutefois que l'Internet a généré dans son sillage divers problèmes relatifs à la sécurité des enfants auxquels il convient de remédier, parce que les implications sont redoutables et parce qu'il est important de communiquer à toutes les personnes concernées que l'Internet est un média dans lequel nous pouvons avoir confiance. Il est tout aussi essentiel de ne pas faire de cette lutte une plateforme permettant de justifier tout autre type d'agression, par exemple contre la liberté de parole, la liberté d'expression ou la liberté d'association.

La nouvelle génération doit avoir confiance dans l'utilisation de l'Internet pour pouvoir continuer de profiter de son développement. Un équilibre doit impérativement être trouvé lorsqu'il s'agit des questions de sécurité des enfants et des adolescents en ligne.

Il importe de discuter ouvertement avec les enfants et les adolescents des risques auxquels ils sont exposés dans le cyberespace et de leur apprendre à gérer ces risques pour autant que ceux-ci soient matérialisés. Ce faisant, nous ne devons ni exagérer les dangers ni générer des craintes non fondées. L'approche qui consiste à présenter exclusivement ou essentiellement les aspects négatifs de la technologie n'aura que très peu de chances d'être prise au sérieux par les enfants et les adolescents qui sont déjà plusieurs centaines de millions à utiliser l'outil au quotidien et à en connaître les tenants et les aboutissants. Les parents et les membres des générations antérieures ont souvent une longueur de retard en la matière. Bien souvent, les jeunes en savent plus sur la technologie et ses possibilités que leurs parents ou leurs enseignants. Mais le savoir n'appelle pas nécessairement la sagesse.

Les gouvernements nationaux ont une obligation de protection des mineurs dans le monde «réel» comme dans le monde «virtuel». Compte tenu de la profonde intégration des nouvelles technologies dans la vie d'un si grand nombre d'enfants et d'adolescents, la distinction rigide entre les événements du «monde réel» et les événements du «monde virtuel» n'a plus lieu d'être, les deux étant aujourd'hui étroitement imbriqués.

Les gouvernements nationaux et les instances de décision ont pour principale mission d'établir un cadre pour une réponse nationale et multinationale appropriée et de maintenir ce cadre. L'industrie Internet et toutes les parties prenantes ont ici un rôle majeur à jouer, entre autres parce que la rapidité avec laquelle la technologie évolue rend les méthodes traditionnelles d'élaboration des lois et des politiques obsolètes. Comme l'explique le présent rapport, les nouvelles technologies ont induit de nouvelles exigences pour les législateurs.

Appendice 1

Abus perpétrés contre les enfants et les adolescents

Dans le cyberespace, les enfants et les adolescents peuvent être exposés à toute une série de contacts non souhaités et inappropriés qui peuvent avoir des conséquences désastreuses sur leur existences. Certains de ces contacts peuvent être de nature sexuelle.

Des études réalisées par *EU Kids Online* en Europe en 2008 révèlent des résultats inquiétants (chiffres médians): 15 à 20% des enfants et des adolescents déclarent avoir fait l'objet de manœuvres d'intimidation, de harcèlement et de traque sur l'Internet; 25% ont reçu des commentaires sexuels non sollicités et 9% ont rencontré des gens dans la vie réelle qu'ils ne connaissaient jusque-là que dans le monde virtuel. Bien qu'ils varient d'une région à l'autre, ces chiffres montrent que le risque est bel et bien réel[26]. Une étude américaine sur l'Internet[27] affirme que 32% des adolescents ont été contactés en ligne par un parfait inconnu, 23% d'entre eux avouent avoir pris peur et avoir ressenti un malaise et, parmi eux, 4% ont fait l'objet de harcèlement sexuel.

Les prédateurs sexuels utilisent l'Internet dans le but d'exploiter des enfants et des adolescents à des fins sexuelles, souvent par la technique du «grooming», une manœuvre qui consiste à gagner la confiance des jeunes en ciblant le ou les sujets qui les touchent particulièrement. Ils parlent souvent de relations sexuelles, diffusent des photos et utilisent un langage explicite pour banaliser la chose, éveiller l'intérêt sexuel et briser la volonté de leurs victimes. Les prédateurs utilisent des cadeaux, de l'argent et même des tickets de transport pour séduire et attirer leurs proies dans des lieux où ils pourront se livrer à des abus sexuels. Les rencontres sont parfois photographiées voire filmées. Bien souvent, les enfants et les adolescents manquent de maturité émotionnelle et d'estime de soi, ce qui les rend particulièrement vulnérables à toute tentative de manipulation et d'intimidation. Ils hésitent également à parler de leurs rencontres aux adultes de peur d'être dans l'embarras ou de se voir refuser l'accès à l'Internet. Dans certains cas, ils subissent les pressions des prédateurs qui les obligent à garder le silence sur leur relation.

Les prédateurs sexuels échangent des informations sur les forums Internet et les chat rooms. Lorsqu'ils communiquent avec les enfants et les adolescents, ils

[26] EU Kids Online Report, *Comparing Children's Online Opportunities and Risks Across Europe*, páginas 29-30, junio de 2008.

[27] *Pew Internet and American Life Project 2007.*

mentent souvent sur leur âge qu'il dise être proche de celui de leur victime et prétendent rechercher l'amitié. Une fois qu'ils ont gagné la confiance de leur interlocuteur, ils se servent de leurs vulnérabilités, telles que la solitude ou le sentiment d'angoisse provoqué par une perte personnelle, pour créer une dépendance émotionnelle. De nombreux rapports font état de cas où des jeunes ayant accepté de rencontrer dans le monde réel une personne qu'ils pensaient être de leur âge et avec laquelle ils conversaient en ligne se sont retrouvés en réalité face à une personne beaucoup plus âgée, de sexe masculin, qui désirait avoir des rapports sexuels avec eux. Certains de ces enfants ont malheureusement été victimes d'une agression sexuelle et dans quelques rares cas, les conséquences se sont révélées bien plus graves.

Il est une tendance particulièrement troublante qui consiste pour un prédateur à diffuser des jeux sexuels mettant en scène des enfants et des adolescents via une webcam en temps réel auprès d'autres prédateurs – souvent pour solliciter leur approbation. Les enfants et les adolescents impliqués souffrent non seulement d'un traumatisme psychologique (et physique) sévère et profond mais sont également à nouveau victime à chaque fois que leur image est diffusée sur l'Internet et qu'ils deviennent des objets de collection pour les autres prédateurs. Ces images sont visionnées et utilisées, commercialisées et parfois vendues sur l'Internet à d'autres prédateurs à la recherche de nouveau matériel pour assouvir leurs fantasmes sexuels. Les victimes sont malheureusement dans l'incapacité de passer à autre chose et de continuer leurs vies même longtemps après les faits, parce qu'elles vivent avec la peur incessante que leur image soit reconnue par d'autres. Plus méprisable encore est le comportement du prédateur qui utilise ces images pour «faire chanter» sa victime en lui demandant de garder le silence et de se plier à tout ce qu'il exigera d'elle.

Appendice 2

Pornographie enfantine: examen de la législation type à l'échelle mondiale

Avec l'aide d'Interpol et de Microsoft, le Centre international pour les enfants disparus et exploités a mené des recherches sur la législation nationale en matière de pornographie enfantine dans les 187 pays membres d'Interpol, et a formulé des recommandations pour des concepts-clés qui, appliqués dans la législation nationale, permettraient de développer une stratégie législative globale destinée à combattre la pornographie enfantine.

Malheureusement, le rapport a révélé[28] que peu de pays disposaient d'une législation appropriée pour combattre la pornographie enfantine à un certain niveau.

Le rapport intégral, actuellement dans sa cinquième édition, peut être consulté à l'adresse www.icmec.org en anglais, arabe, coréen, espagnol, français, portugais, russe, thaï et turque[29].

La liste ci-dessous énumère les pays membres d'Interpol en indiquant le statut de leur législation en matière de pornographie enfantine.

[28] Les résultats obtenus sont les suivants:

- ✓ 29 pays seulement ont une législation appropriée pour combattre les délits de pornographie enfantine (cinq pays membres satisfont à tous les critères énoncés ci-dessus et 24 pays membres satisfont à tous les critères, à l'exception du dernier, portant sur le signalement par les FAI);
- ✓ 93 pays n'ont aucune législation abordant spécifiquement le problème de la pornographie enfantine.

Des pays restants qui ont une législation abordant spécifiquement le problème de la pornographie enfantine:

- 54 pays n'offrent pas de définition de la pornographie enfantine dans leur législation nationale;
- 24 pays ne prévoient explicitement aucune disposition pour les délits assistés par ordinateur; et
- 36 pays ne criminalisent pas la possession de la pornographie enfantine, indépendamment de l'intention de diffuser.

[29] www.icmec.org

Examen de la législation à l'échelle mondiale

(Réimprimé avec la permission du Centre international pour les enfants disparus et exploités)

✗ = No ✓ = Oui

Pays	Législation spécifique à la pornographie enfantine[30]	«Pornographie enfantine» définie	Délits assistés par ordinateur[31]	Possession simple[32]	Signalement par les FAI[33]
Afganistan	✗	✗	✗	✗	✗
Albanie	✗	✗	✗	✗	✗
Algérie	✗	✗	✗	✗	✗
Andorre	✓	✗	✗	✓	✗
Angola	✗	✗	✗	✗	✗

[30] Aux fins de ce rapport, nous avons examiné les lois spécifiques qui interdisent et/ou sanctionnent les délits de pornographie enfantine. La législation du travail seule qui interdit tout simplement les «pires formes de travail des enfants», y compris la pornographie enfantine, n'est pas considérée comme une «législation spécifique à la pornographie enfantine».
Par ailleurs, les pays dans lesquels il existe une interdiction générale de la pornographie, regroupant enfants et adultes, ne sont pas considérés comme ayant une «législation spécifique à la pornographie enfantine», à moins que des peines accrues ne soient prévues pour les délits commis contre un enfant victime.

[31] Pour qualifier un délit de «délit assisté par ordinateur», nous avons guetté toute mention spécifique d'un ordinateur, d'un système informatique, d'Internet ou tout langage similaire (même s'il s'agit d'une «image informatique» ou de quelque chose d'analogue dans la définition de la «pornographie enfantine»). Si un autre langage est utilisé dans la législation nationale, une note de page de page explicative est fournie.

[32] La «possession simple» dans ce rapport fait référence à la possession, quelle que soit l'intention de distribution.

[33] Même si certains pays ont des lois générales de signalement (c'est-à-dire, toute personne qui prend connaissance d'un crime doit le signaler aux autorités appropriées), seuls les pays qui exigent précisément que les FAI signalent les cas de pornographie enfantine soupçonnés à la police (ou à un autre organisme mandaté) sont considérés comme ayant des lois sur le signalement par les FAI. Il est important de constater que certaines lois nationales (essentiellement à l'intérieur de l'Union européenne) contiennent également des dispositions limitant la responsabilité criminelle d'un FAI à condition que le FAI retire le contenu illégal une fois qu'il a pris connaissance de sa présence; toutefois, une telle législation n'est pas incluse dans cette section.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Antigua-et-Barbuda	✗	✗	✗	✗	✗
Argentina	✓	✓	✓	✗	✗
Arménie	✓	✗	✓	✗	✗
Aruba	✓	✗	✓	✓	✗
Australie	✓	✓	✓	✓	✓
Autriche	✓	✓	✓[34]	✓	✗
Azerbaïdjan	✗	✗	✗	✗	✗
Bahamas	✗	✗	✗	✗	✗
Bahreïn	✗	✗	✗	✗	✗
Bangladesh	✗	✗	✗	✗	✗
Barbade	✓	✗	✗	✓	✗

[34] La Section 207a(1)(3) du Code pénal autrichien criminalise la «mise à la disposition **de toute autre manière…** d'une représentation pornographique d'un mineur.» *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Bélarus	✓	✗	✗	✗	✗
Belgique	✓	✓	✓[35]	✓	✓
Belize	✗	✗	✗	✗	✗
Bénin	✗	✗	✗	✗	✗
Bhoutan	✓	✗	✓[36]	✗	✗
Bolivie	✗	✗	✗	✗	✗
Bosnie-Herzégovine	✓	✗	✓[37]	✓	✗
Botswana	✗	✗	✗	✗	✗
Brésil	✓	✓	✓	✓	✗

[35] Article 383bis du Code pénal belge, tel que modifié le 1er avril 2001, criminalise, entre autres, la diffusion de la pornographie enfantine, incluant ainsi la diffusion par ordinateur. Lettre de Jan Luykx, chef de mission adjoint, Ambassade de Belgique, Washington, D.C., à Ernie Allen, Président-directeur général, Centre international pour les enfants disparus et exploités (24 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[36] Selon l'article 225(b) du Code pénal du Bhoutan, «[un] accusé est coupable de la défense de la pédophilie si l'accusé… vend, fabrique, diffuse ou **échange autrement** du matériel contenant toute représentation d'un enfant engagé dans des contacts sexuels.» *Emphase supplémentaire.*

[37] Les articles 189 et 211 du Code pénal de la Bosnie-Herzégovine font allusion à d'«autre matériel pornographique» en plus de photos et de bandes audiovisuelles.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Brunéi	✓	✗	✓	✗	✗[38]
Bulgarie	✓	✗	✓[39]	✓	✗
Burkina Faso	✗	✗	✗	✗	✗
Burundi	✗	✗	✗	✗	✗
Cambodge	✗	✗	✗	✗	✗
Cameroun	✗	✗	✗	✗	✗

[38] Même s'il n'y a pas d'exigence de signalement obligatoire spécifique aux FAI, aux termes des lois de Brunei, tous les FAI et Fournisseurs de Contenu Internet (FCI) détenant une licence accordée dans le cadre de la *Broadcasting (Class Licence) Notification* de 2001 (notification de licence de catégorie de radiodiffusion) doivent se conformer au Code de bonne pratique établi par la loi sur la radiodiffusion (*Broadcasting Act*) (Cap 181). Les FAI et FCI doivent prouver au Ministre chargé des questions de radiodiffusion qu'ils ont pris des mesures responsables pour remplir cette exigence. Aux termes de la loi sur la radiodiffusion, ce Ministre a le pouvoir d'imposer des sanctions. Le contenu qui ne doit pas être autorisé comprend, entre autres, tout matériel qui représente ou favorise la pédophilie.
Le titulaire de la licence doit retirer ou interdire la diffusion partielle ou intégrale d'un programme faisant partie de ses services si le Ministre lui fait savoir que la diffusion partielle ou intégrale du programme est contraire au Code de bonne pratique applicable au titulaire de la licence ou si le programme va à l'encontre de l'intérêt public, de l'ordre public ou de l'harmonie nationale, ou est contraire au bon goût ou à la bienséance.
Le titulaire de la licence doit également coopérer avec le Ministre chargé des questions de radiodiffusion en cas d'enquête sur toute violation de sa licence ou toute infraction prétendue à toute loi commise par le titulaire ou toute autre personne; et il doit produire également les informations, enregistrements, documents, données ou autre matériel requis par le Ministre aux fins de l'enquête. Courriel de Salmaya Salleh, deuxième secrétaire de l'Ambassade de Brunei à Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (21 mars 2006) (archives du Centre international pour les enfants disparus et exploités).

[39] L'article 159(3) du Code pénal bulgare, lu en association avec l'Article 159(1), criminalise, entre autres, les «œuvres **diffusées autrement** et contenant du matériel pornographique [enfantin]». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Canada	✓	✓	✓	✓	✗ [40]
Cap-Vert	✓	✗	✗	✗	✗
République centrafricaine	✗	✗	✗	✗	✗
Tchad	✗	✗	✗	✗	✗
Chili	✓	✓	✓	✗	✗

[40] Même s'il n'y a pas d'exigence de signalement obligatoire spécifique aux FAI, les FAI au Canada collaborent avec la police et travaillent étroitement entre eux pour faciliter le signalement du matériel incriminé en cas de détection. Le droit pénal canadien utilise une définition très large du terme «pornographie enfantine», qui élargit son champ d'action avec une série de délits supplémentaires. Les délits spécifiques de transmission, d'offre et d'accès ont été ajoutés en 2002 afin de prendre en compte le contexte Internet et s'appliquent aux activités des FAI. Le Canada a également introduit dans cette même législation une disposition de «notification et retrait» pour le matériel de pornographie enfantine découvert sur Internet. La détermination des peines pour délits de pornographie enfantine a été assortie en 2005 des éléments suivants: imposition de peines minimales, augmentation des peines maximales dans les procédures sommaires, de 6 à 18 mois d'emprisonnement, établissement de la dénonciation et de la dissuasion comme objectifs prioritaires dans tous les cas impliquant des abus sur des enfants, et considérant les abus sur des enfants comme facteurs aggravants dans la détermination des peines. Outre les protections détaillées décrites dans le droit pénal, le Canada dispose également d'une ligne d'urgence publique nationale réservée au signalement de l'exploitation sexuelle d'enfants sur Internet (www.cybertip.ca) qui effectue un triage de ces signalements pour les agents de la police. De plus, Cybertip.ca tient à jour une banque de données «*Cleanfeed Canada*» qui bloque pour environ 90% des abonnés canadiens l'accès aux sites connus de pornographie enfantine susceptibles d'être hors d'atteinte de poursuites canadiennes. Par ailleurs, le Canada dispose d'une stratégie nationale en matière de protection des enfants contre l'exploitation sexuelle sur Internet, avec pour composante-clé le Centre national de coordination de l'exploitation d'enfants (*National Child Exploitation Coordination Centre*, ou Centre). Le Centre, situé auprès de la Gendarmerie royale du Canada, coordonne les enquêtes intérieures et à l'étranger sur l'exploitation sexuelle d'enfants en ligne, fournit des formations aux agents de police canadiens, et sert de centre d'échanges pour les rapports reçus de Cybertip.ca. Résumé de la lettre de Carole Morency, avocate générale, section de la politique en matière de droit pénal, département canadien de la Justice, à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (24 juin 2008) (l'intégralité de la lettre figure aux archives du Centre international pour les enfants disparus et exploités).

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Chine[41]	✓[42]	✗	✓[43]	✗	✗
Colombie	✓	✓	✓	✗	✓
Comores	✗	✗	✗	✗	✗
Congo	✗	✗	✗	✗	✗
Costa Rica	✓	✓	✗	✓	✗
Côte d'Ivoire	✗	✗	✗	✗	✗
Croatie	✓	✗	✓	✓	✗

[41] La législation de Hong Kong relative à la pornographie enfantine diffère de celle de la Chine. Législation de Hong Kong:
- définit la pornographie enfantine;
- criminalise les délits assistés par ordinateur; et
- criminalise la simple possession de matériel de pornographie enfantine.

[42] Même si la Chine ne dispose pas de législation spécifique sur la pornographie enfantine, le Code criminel interdit de manière générale tout matériel obscène et pornographique. En 2004, en vue de mieux protéger les mineurs, la Cour suprême du peuple et le Protectorat suprême du peuple ont promulgué une «Interprétation de plusieurs questions concernant l'application des lois pour traiter des cas criminels liés à la production, reproduction, publication, vente ou diffusion d'informations électroniques pornographiques via Internet, les terminaux de communication mobile et les stations radio.» L'article 6 de cette interprétation stipule explicitement que «toute personne qui diffuse, reproduit, publie ou vend des informations électroniques pornographiques qui représentent les comportements sexuels d'adolescents de moins de 18 ans ou qui fournit des liens directs, sur le serveur Internet ou les sites web qu'elle gère ou utilise ou dont elle est le propriétaire, à ces informations électroniques, sachant que ces informations représentent les comportements sexuels d'adolescents de moins de 18 ans, sera sévèrement punie conformément à l'article 363 du Droit pénal réglementant la punition des crimes de production, de reproduction, de publication, de vente ou de diffusion de matériel pornographique ou à l'article 364 réglementant la punition de crimes de diffusion de matériel pornographique dans des circonstances graves». Courriel de Chen Feng, agent de liaison avec la police, Ambassade de la République populaire de Chine, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre International pour les enfants disparus et exploités (17 mars 2006) (archives du Centre international pour les enfants disparus et exploités).

[43] L'interprétation de la Cour suprême et du Protectorat suprême du peuple de 2004 s'applique aux délits assistés par ordinateur.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Cuba	✗	✗	✗	✗	✗
Chypre	✓	✓	✓	✓	✗
République tchèque	✓	✗	✓	✓	✗[44]
République démocratique du Congo	✗	✗	✗	✗	✗
Danemark	✓	✓	✓[45]	✓	✗
Djibouti	✗	✗	✗	✗	✗
Dominique	✗	✗	✗	✗	✗
République dominicaine	✓	✓	✓	✓	✗
Équateur	✓	✗	✗	✗	✗
Egypte	✓	✗	✓	✓	✗

[44] Même si la loi tchèque ne comporte aucune exigence de signalement par les FAI, le Plan national tchèque sur la lutte contre l'exploitation sexuelle commerciale des enfants, disponible en ligne à l'adresse: www.mvcr.cz/prevence/priority/kszd/en_tab.html, désigne le Ministère des transports et des communications et le Ministère de l'intérieur comme les organismes nationaux chargés de préciser les obligations réglementaires des fournisseurs d'accès à Internet (voir l'Acte sur les télécommunications (N° 151/2000)), concernant l'enregistrement des données nécessaires sur les sites web illégaux et la transmission de ces données à la police tchèque. Le résultat attendu de cette mesure sera de conserver les «éléments de preuve incriminant ceux qui propagent du matériel de pornographie enfantine sur Internet».

[45] La Section 235 du Code pénal danois criminalise, entre autres, la diffusion et la possession d'«autres… reproductions visuelles» de matériel pornographique concernant les enfants âgés de moins de 18 ans.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
El Salvador	✓	✗	✓	✓	✗
Guinée équatoriale	✗	✗	✗	✗	✗
Érythrée	✗	✗	✗	✗	✗
Estonie	✓	✗	✓[46]	✓	✗
Éthiopie	✗	✗	✗	✗	✗
Fiji	✗	✗	✗	✗	✗
Finlande	✓	✓	✓[47]	✓	✗
France	✓	✓	✓	✓	✓
Gabon	✗	✗	✗	✗	✗
Gambie	✓	✗	✗	✗	✗
Géorgie	✓	✓	✗	✗	✗

[46] Les articles 177 et 178 du Code pénal estonien criminalisent l'emploi d'un mineur dans d'«autres travaux» ou l'emploi de «tout autre moyen» pour fabriquer, conserver, transmettre, afficher ou fournir du matériel de pornographie enfantine.

[47] Le Chapitre 17, Section 18 de l'Acte criminel finlandais criminalise «toute personne qui… diffuse autrement des images ou des enregistrements visuels obscènes représentant des enfants».

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Allemagne	✓	✓	✓	✓	✗[48]
Ghana	✗	✗	✗	✗	✗
Grèce	✓	✓	✓[49]	✓	✗
Grenade	✗	✗	✗	✗	✗
Guatemala	✓	✗	✗	✗	✗
Guinée	✗	✗	✗	✗	✗
Guinée-Bissau	✗	✗	✗	✗	✗
Guyana	✗	✗	✗	✗	✗
Haïti	✗	✗	✗	✗	✗
Honduras	✓	✓	✓	✓	✗

[48] Même si un FAI n'a pas d'obligation explicite en matière de signalement à la police ou à un autre organisme mandaté, dans la plupart des cas, les FAI déposeront des rapports auprès de la police. Un FAI qui a connaissance de matériel de pornographie enfantine posté sur ses sites web et qui n'efface pas ce contenu illégal est passible de poursuites. Entre autres facteurs, on essaie de déterminer si le FAI pouvait raisonnablement détecter les données et les supprimer ou de les bloquer, car il y a de nombreux FAI en Allemagne qui offrent de grandes capacités de stockage à des fins commerciales. Courriel de Klaus Hermann, conseiller/agent de liaison de l'ambassade d'Allemagne à Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre International pour les enfants disparus et exploités (9 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[49] L'article 348a du Code pénal grec criminalise divers délits de pornographie enfantine, y compris la possession, l'achat, le transfert et la vente de matériel de pornographie enfantine «de quelque manière que ce soit».

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Hongrie	✓	✓	✓[50]	✓	✗
Islande	✓	✗	✓[51]	✓	✗
Inde	✓	✗	✓	✓	✗
Indonésie	✗	✗	✗	✗	✗
Iran	✗	✗	✗	✗	✗
Iraq	✗	✗	✗	✗	✗
Irlande	✓	✓	✓	✓	✗
Israël	✓	✓	✓	✓	✗
Italie	✓	✓	✓	✓	✗
Jamaïque	✗	✗	✗	✗	✗
Japon	✓	✓	✓	✗	✗

[50] En vertu de la Section 195/A(3) du Code pénal hongrois, une personne qui fabrique, diffuse ou échange des images pornographiques d'un mineur à l'aide de vidéos, films, photos ou «par tout autre moyen», ou qui met de telles images à la disposition du public, commet un acte délictueux grave. Par ailleurs, selon une décision récente de la Cour d'appel hongroise (n° BH 133/2005), les références à «tout autre moyen» et à «la mise à la disposition du public» incluent la diffusion via Internet. Lettre de Viktor Szederkényi, chef de mission adjoint, Ambassade de la République de Hongrie, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre International pour les Enfants Disparus et Exploités (6 février 2006) (archives du Centre International pour les Enfants Disparus et Exploités).

[51] L'article 210 du Code pénal de l'Islande criminalise la «possession de photos, de films ou d'**articles comparables** représentant les enfants d'une manière sexuelle ou obscène». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Jordanie	✗	✗	✗	✗	✗
Kazakhstan	✓	✗	✗	✗	✗
Kenya	✗	✗	✗	✗	✗
Corée	✓	✓	✓	✗	✗
Koweït	✗	✗	✗	✗	✗
Kirghizistan	✓	✗	✗	✗	✗
Laos	✗	✗	✗	✗	✗
Lettonie	✓	✗	✓[52]	✗	✗
Liban	✗	✗	✗	✗	✗
Lesotho	✗	✗	✗	✗	✗
Libéria	✗	✗	✗	✗	✗
Libye	✗	✗	✗	✗	✗

[52] L'article 166(2) du Droit criminel letton criminalise «l'importation, l'exposition publique, la publicité ou **toute autre diffusion** de matériel… pornographique lié à ou représentant l'abus sexuel d'enfants». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Liechtenstein	✓	✗	✓	✓	✗[53]
Lituanie	✓	✗	✗	✓	✗
Luxembourg	✓	✗	✓[54]	✓	✗
Macédoine	✓	✗	✓[55]	✗	✗
Madagascar	✓	✗	✓[56]	✗	✗
Malawi	✗	✗	✗	✗	✗
Malaisie	✗	✗	✗	✗	✗
Maldives	✗	✗	✗	✗	✗
Mali	✓	✗	✗	✗	✗
Malta	✓	✗	✓	✓	✗

[53] Même si le Code pénal du Liechtenstein ne comporte aucune mention précise de signalement par les FAI, dans l'avant-projet de la nouvelle loi sur les enfants et les jeunes (*Children and Youth Act*), une exigence de signalement est prévue et s'applique à «toute personne qui prend connaissance d'une menace pesant sur le bien-être d'un enfant ou d'une jeune personne». Courriel de Claudia Fritsche, ambassadrice, Ambassade du Liechtenstein, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (7 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[54] L'article 383 du Code pénal du Luxembourg criminalise non seulement la fabrication et la possession (à des fins commerciales, de diffusion ou de présentation publique) d'«œuvres écrites ou imprimées, d'images, de photos, de films ou **autres objets** d'une nature pornographique», mais aussi la commission d'une variété de délits liés à la pornographie enfantine «de quelque façon que ce soit». *Emphase supplémentaire.*

[55] L'article 193(3) du Code pénal de la Macédoine criminalise l'abus d'un «jeune» dans la «production [d'autres] objets à contenu pornographique».

[56] L'article 346 du Code pénal du Madagascar criminalise le recours à «tout moyen» pour diffuser du matériel de pornographie enfantine.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Iles Marshall	✗	✗	✗	✗	✗
Mauritanie	✗	✗	✗	✗	✗
Maurice	✓	✗	✓	✗	✗
Mexique	✓	✓	✓	✗	✗
Moldavie	✓	✗	✗	✓	✗
Monaco	✗	✗	✗	✗	✗
Mongolie	✗	✗	✗	✗	✗
Monténégro	✓	✗	✓[57]	✗	✗
Maroc	✓	✗	✗	✓	✗
Mozambique	✗	✗	✗	✗	✗
Myanmar	✓	✗	✗	✗	✗
Namibie	✗	✗	✗	✗	✗
Nauru	✗	✗	✗	✗	✗

[57] L'article 211(2) du Code pénal de Monténégro criminalise l'«exploitation d'un enfant pour la production d'images, de matériel audiovisuel ou de **tout autre article** à contenu pornographique». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Népal	✓	✗	✗[58]	✗	✗
Pays-Bas	✓	✓	✓	✓	✗[59]
Antilles néerlandaises	✗[60]	✗	✗[61]	✗[62]	✗
Nouvelle-Zélande	✓	✓	✓	✓	✗
Nicaragua	✗	✗	✗	✗	✗
Niger	✗	✗	✗	✗	✗
Nigeria	✗	✗	✗	✗	✗
Norvège	✓	✓	✓	✓	✗
Oman	✗	✗	✗	✗	✗
Pakistan	✗	✗	✗	✗	✗

[58] Même s'il ne s'agit pas spécifiquement de la pornographie enfantine, la Section 47 de l'Ordonnance sur les transactions électroniques (*Electronic Transaction Ordinance*) de 2004 interdit la publication ou l'affichage par ordinateur, sur Internet ou sur tout autre support électronique, de tout matériel dont la publication ou l'affichage est interdit par la loi parce qu'il va à l'encontre de la moralité et de la décence publiques.

[59] Même si les FAI n'ont aucune obligation légale ou contractuelle de rapporter les cas de pornographie enfantine soupçonnés à la police, les FAI aux Pays-Bas ont tendance à signaler immédiatement à la police leurs découvertes en matière de pornographie enfantine, et les FAI retirent le contenu du site web concerné. Par ailleurs, à la demande de la police, les FAI fournissent leurs journaux concernant le ou les sites web douteux. Courriels de Richard Gerding, conseiller auprès de la Police et des affaires judiciaires, Ambassade royale des Pays-Bas, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (8 février 2006) (archives du centre international pour les enfants disparus et exploités).

[60] Même si la législation spécifique à la pornographie enfantine n'existe pas encore, un comité a été établi pour passer en revue le Code pénal actuel des Antilles néerlandaises. Une législation spécifique portant sur la pornographie enfantine sera introduite (Article proposé 2.13.4). Courriel de Richard Gerding, conseiller auprès de la Police et des affaires judiciaires, Ambassade royale des Pays-Bas, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre International pour les enfants disparus et exploités (22 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[61] L'article proposé 2.13.4 criminaliserait tout délit assisté par ordinateur.

[62] L'article proposé 2.13.4 criminaliserait la simple possession.

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Panama	✓	✓	✓	✓	✗[63]
Papouasie-Nouvelle-Guinée	✓	✗	✗	✓	✗
Paraguay	✓	✗	✗	✓	✗
Pérou	✓	✓	✓	✓	✗
Philippines	✓	✗	✗	✗	✗
Pologne	✓	✗	✗	✓	✗
Portugal	✓	✗	✓[64]	✓	✗
Qatar	✓	✗	✓[65]	✗	✗
Roumanie	✓	✓	✓	✓	✗

[63] Même s'il n'existe aucune exigence de signalement obligatoire spécifique aux FAI, l'article 231-I du Code pénal panaméen établit que toute personne qui a connaissance de l'emploi de mineurs aux fins de la pornographie, que ces informations aient été obtenues par le biais de ses fonctions, son emploi, son commerce, sa profession ou par tout autre moyen, et qui ne le signale pas aux autorités, sera tenue responsable et condamnée à la prison. Par contre, le dénonciateur ne pourra pas être poursuivi dans le cadre de son rapport aux autorités si le crime (pornographie enfantine ou activité sexuelle) ne peut être prouvé après le rapport. Courriel d'Isabel Fernández, Ambassade du Panama, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (12 avril 2006) (archives du Centre international pour les enfants disparus et exploités).

[64] On peut déduire de l'article 172 du Code pénal portugais que la tournure «par tout moyen» permet à un procureur de considérer les technologies de l'information et des communications comme un moyen de commettre un crime par la diffusion d'images, de sons ou de films qui montrent des mineurs de moins de 14 ans participant à des actes sexuels. Lettre de Pedro Catarino, ambassadeur, Ambassade du Portugal, Washington, D.C., à Ernie Allen, président directeur général du Centre international pour les enfants disparus et exploités (22 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[65] L'article 292 du Code pénal du Qatar mentionne spécifiquement «livres, publications, **autres documents écrits,** images, photos, films, symboles ou **autres articles**». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Russie	✓	✗	✗	✗	✗
Rwanda	✗	✗	✗	✗	✗
Saint Kitts & Nevis	✗	✗	✗	✗	✗
Sainte-Lucie	✗	✗	✗	✗	✗
Saint-Vincent-et-les-Grenadines	✗	✗	✗	✗	✗
Saint-Marin	✓	✗	✓	✗	✗
Sao Tomé-et-Principe	✗	✗	✗	✗	✗
Arabie saoudite	✗	✗	✗	✗	✗
Sénégal	✗	✗	✗	✗	✗
Serbie	✓	✗	✓[66]	✗	✗
Seychelles	✗	✗	✗	✗	✗

[66] L'article 111a du Code pénal serbe criminalise la prise d'une «photo, la réalisation d'un film ou la fabrication de **toute autre image**» d'un mineur en vue de produire un article à contenu pornographique. Par ailleurs, l'article 185 criminalise le recours à un mineur pour la production «d'images, de matériel audiovisuel ou de tout autre article à contenu pornographique». *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Sierra Leone	✗	✗	✗	✗	✗
Singapour	✗	✗	✗	✗	✗
République slovaque	✓	✓	✓	✓	✗
Eslovénie	✓	✓	✓[67]	✗	✗
Somalie	✗	✗	✗	✗	✗
Afrique du Sud	✓	✓	✓	✓	✓
Espagne	✓	✗	✓[68]	✓	✗
Sri Lanka	✓	✗	✗	✓	✗
Soudan	✗	✗	✗	✗	✗
Surinam	✗	✗	✗	✗	✗
Swaziland	✗	✗	✗	✗	✗

[67] L'article 187(2) du Code pénal de Slovénie criminalise l'abus d'un mineur «en vue de produire des images, du matériel audiovisuel ou **tout autre article** de nature pornographique»; l'article 187(3) criminalise les actions de toute personne qui «produit, diffuse, vend, importe, exporte,… ou fournit [du matériel pornographique représentant des mineurs] **de toute autre manière**, ou qui possède ce type de matériel et a l'intention de le produire, diffuser, vendre, importer, exporter ou fournir **de toute autre manière**.» *Emphase supplémentaire.*

[68] L'article 189(1)(a) du Code pénal espagnol criminalise l'emploi d'un mineur «pour préparer tout type de matériel pornographique»; l'article 189(1)(b) criminalise la production, la vente, la diffusion, l'exposition ou la facilitation de la production, de la vente, de la diffusion ou de l'exposition, de «**tout type**» de pornographie enfantine par «tout moyen»; et l'article 189(7) reprend les formulations «tout type» et «tout moyen» utilisées auparavant. *Emphase supplémentaire.*

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Suède	✓	✗	✓[69]	✓	✗[70]
Suisse	✓	✓	✓	✓	✗
Syrie	✗	✗	✗	✗	✗
Tadjikistan	✓	✗	✗	✗	✗
Tanzanie	✓	✗	✗	✗	✗
Thaïlande	✗	✗	✗	✗	✗
Timor Leste	✗	✗	✗	✗	✗
Togo	✗	✗	✗	✗	✗
Tonga	✓	✓	✓	✓	✗
Trinité-et-Tobago	✗	✗	✗	✗	✗

[69] La législation criminelle suédoise est, en principe, formulée de manière à être applicable, indépendamment des préalables techniques. Il en va de même pour la criminalisation de la pornographie enfantine et, par conséquent, le Chapitre 16, Section 10a, du code pénal suédois s'étend aux délits assistés par ordinateur. Lettre d'Anette Nilsson, première secrétaire, Ambassade de Suède, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (23 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[70] En 1998, la Suède a promulgué une loi sur la responsabilité légale en matière de babillards électroniques (*Bulletin Board System* (BBS) *Liability Act* (1998:112)), dont le but consiste à empêcher la propagation de matériel de pornographie enfantine en obligeant les fournisseurs de babillards à en surveiller le contenu. Les fournisseurs de babillards sont également tenus de supprimer ou d'empêcher d'une manière ou d'une autre, la diffusion de messages à contenu criminel, y compris ceux comportant du matériel de pornographie enfantine. Lettre d'Anette Nilsson, première secrétaire, Ambassade de Suède, Washington, D.C., à Jessica Sarra, directrice des opérations internationales, Centre international pour les enfants disparus et exploités (23 février 2006) (archives du Centre international pour les enfants disparus et exploités).

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Tunisie	✓	✗	✓[71]	✗	✗
Turquie	✓	✗	✗	✓	✗
Turkménistan	✗	✗	✗	✗	✗
Ouganda	✗	✗	✗	✗	✗
Ukraine	✓	✗	✓	✗	✗
Émirats arabes unis	✗	✗	✗	✗	✗
Royaume-Uni[72]	✓	✓	✓	✓	✗[73]
États-Unis	✓	✓	✓	✓	✓
Uruguay	✓	✗	✓[74]	✗	✗
Ouzbékistan	✗	✗	✗	✗	✗

[71] L'article 234 du Code pénal tunisien criminalise, entre autres, l'emploi de «tout enregistrement visuel ou de toute photographie» montrant des images pornographiques d'enfants.

[72] Aux fins de ce rapport, le Royaume-Uni comprend l'Angleterre et le Pays de Galles.

[73] Le Royaume-Uni a mis en place une procédure volontaire de «notification et de retrait» (*notice and takedown*) surveillée par l'*Internet Watch Foundation* ou l'IWF, un organisme indépendant de régulation d'Internet, financé par l'industrie, et soutenu par la police et le gouvernement. Les FAI du Royaume-Uni «retirent» les images pornographiques enfantines après avoir été notifiés de leur présence par l'IWF. S'ils ne le font pas, ils pourraient être passibles de poursuites. Lettre de Tony Lord, premier secrétaire, Justice et affaires domestiques, ambassade de Grande-Bretagne, Washington, D.C., à Ernie Allen, président-directeur général, Centre International pour les enfants disparus et exploités (9 février 2006) (archives du Centre international pour les enfants disparus et exploités).

[74] La loi 17.815 de la République orientale de l'Uruguay criminalise certains délits de pornographie enfantine, indépendamment de la manière dont ils sont commis (par exemple, Article 1: «qui fait ou fabrique de quelque manière que ce soit du matériel de pornographie enfantine»; Article 2: «qui facilite de quelque manière que ce soit, la commercialisation, la diffusion, l'exposition, la conservation ou l'acquisition de matériel de pornographie enfantine»).

Pays	Législation spécifique à la pornographie enfantine	«Pornographie enfantine» définie	Délits assistés par ordinateur	Possession simple	Signalement par les FAI
Vatican	✗[75]	✗	✗	✗	✗[76]
Venezuela	✓	✓	✓	✗	✗
Viet Nam	✗	✗	✗	✗	✗
Yémen	✗	✗	✗	✗	✗
Zambie	✗	✗	✗	✗	✗
Zimbabwe	✗	✗	✗	✗	✗

[75] En l'absence de législation spécifique en matière de pornographie enfantine, les cas sont renvoyés au système judiciaire italien à la demande du Saint-Siège.

[76] «Le Saint-Siège ne dispose pas de fournisseur d'accès Internet externe et la navigation à partir du fournisseur interne est équipée de filtres empêchant non seulement l'accès à tous sites de pornographie enfantine, mais aussi la distribution de matériel pornographique. Comme le site Web du Saint-Siège est institutionnel, il ne contient que les matières inhérentes à sa mission.» Lettre de l'archevêque Pietro Sambi, nonce apostolique, nonciature des États-Unis d'Amérique, à Ernie Allen, président-directeur général, Centre international pour les enfants disparus et exploités (5 juin 2006) (archives du Centre international pour les enfants disparus et exploités).

Appendice 3

Logiciels de contrôle parental

Il existe sur le marché de nombreux packs logiciels et dispositifs techniques qui permettent de supprimer les contenus et contacts non sollicités ou non désirés, de limiter les temps de connexion à l'Internet et de restreindre le nombre d'applications supportées sur un ordinateur ou un équipement spécifique. Certains systèmes d'exploitation incluent ces outils dans leurs fonctionnalités de base, répondant ainsi aux exigences contenues dans les principaux messages de sécurité véhiculés dans toutes les régions du monde par les campagnes relatives à la sécurité sur l'Internet. De telles applications sont utilisées dans les écoles et dans les bibliothèques municipales. Elles sont également très proches de celles employées par les patrons d'entreprise sur leurs réseaux internes pour limiter l'usage non approprié ou non professionnel de l'Internet pendant les heures de travail.

Les performances de ces logiciels de sécurité enfant sont parfois très inégales, et des efforts ont été déployés dans certains pays pour introduire un «label» visant à fournir aux parents, aux enseignants ainsi qu'aux enfants et aux adolescents une assurance qualité minimale pour les aider à choisir un programme correspondant à leurs besoins, tout à la fois efficace et convivial.

Il est important de rappeler toutefois que ces équipements et ces logiciels seront tôt ou tard amenés à défaillir. Les parents, les enseignants, les enfants et les adolescents ne doivent donc pas leur faire une confiance aveugle, mais toujours les considérer comme un complément à d'autres programmes d'éducation et de sensibilisation visant à donner aux enfants et aux adolescents les moyens d'éviter et, le cas échéant, de combattre les menaces en ligne.

Exemples de packs logiciels assurant la sécurité des enfants:

Produits gratuits

1. *K9 Web Protection* (http://www.k9webprotection.com/)
2. *SafeFamilies* (http://www.safefamilies.org/download.php)
3. *File Sharing Sentinel* (http://www.akidthaine.com/)
4. *B-Gone* (http://support.it-mate.co.uk/?mode=Products&p= bgone)

5. Les dernières versions de Windows et Mac OS incluent certaines applications qui peuvent être utilisées sans frais

Produits payants

- *Net Nanny Parental Controls*
- *Safe Eyes*
- *CYBERsitter*
- *WiseChoice.net*
- *CyberPatrol*
- *MaxProtect*
- *FilterPak*
- *Netmop*
- *imView*
- *McAfee Parental Controls*
- *Norton Parental Controls*
- *Child Safe*
- *ContentProtect Security Appliance*
- http://www.cybersentinel.co.uk/

Une liste plus détaillée des produits gratuits et payants figure à l'adresse www.getnetwise.org

Appendice 4

Développer une stratégie nationale

Le développement de l'Internet a favorisé la perpétration d'une série de crimes contre les enfants et les adolescents, par exemple via les web cams et les chat rooms, qui auraient été impossibles si l'Internet n'était pas devenu un produit de consommation de masse. L'Internet a également joué un rôle particulier dans l'extension des possibilités offertes en matière de diffusion du matériel de pornographie enfantine. Lorsqu'ils abordent la problématique de la sécurité en ligne des enfants et des adolescents, les décideurs ont donc intérêt à prêter une attention particulière à certaines ou à l'ensemble des actions suivantes:

1. Criminaliser les tentatives d'attirance à des fins d'abus sexuel («*grooming*») ou toute autre forme de sollicitation des mineurs à distance en vue de contacts ou de rapports sexuels inappropriés.

2. Criminaliser la possession, la production et la distribution de matériel de pornographie enfantine, indépendamment de l'intention de le diffuser ou non.

3. Introduire des mesures supplémentaires en vue de perturber ou de réduire le trafic de matériel de pornographie enfantine, par exemple en instaurant une hotline nationale ou en déployant des mesures visant à bloquer l'accès aux sites web et aux *Usenet Newsgroup* réputés contenir ou faire la publicité de la pornographie enfantine.

4. Veiller à la mise en place de procédures nationales permettant d'avoir l'assurance que tout le matériel de pornographie enfantine trouvé dans un pays a transité via une ressource nationale centralisée.

5. Développer des stratégies de lutte contre la demande de pornographie enfantine, notamment auprès des personnes reconnues coupables de délits. Il est important de faire comprendre que le crime n'est pas sans victime: les enfants sont exploités pour produire du matériel qui est ensuite visionné, et celui qui consulte ou télécharge ce matériel participe directement à l'exploitation de l'enfant mis en scène et encourage de surcroît l'exploitation ultérieure d'autres enfants qui feront l'objet de nouvelles images.

6. Sensibiliser au fait qu'un enfant ne peut pas consentir à être exploité sexuellement, que ce soit dans le cadre de la production de matériel de pornographie enfantine ou d'une autre manière. Encourager les utilisateurs de matériel de pornographie enfantine à rechercher de l'aide et, dans le même temps, leur faire comprendre qu'ils sont pénalement responsables des activités illicites qu'ils ont entrepris ou qu'ils entreprennent.

7. Veiller à ce que les stratégies policières de prévention criminelle, les programmes scolaires et les plans sociaux comportent des sections sur la cybersécurité ainsi que sur les risques liés au comportement des prédateurs en ligne et fournissent des conseils adaptés à chaque âge.

8. Envisager d'autres stratégies de lutte contre la demande de pornographie enfantine. Certains pays, par exemple, tiennent un registre des agresseurs sexuels ayant fait l'objet d'une condamnation. Les tribunaux ont prononcé des décisions judiciaires interdisant à ces agresseurs d'utiliser l'Internet en général ou seuls certains sites fréquentés par les enfants et les adolescents. Le problème rencontré jusqu'à présent est celui de leur application. Certains pays envisa-

gent toutefois d'inclure la liste des agresseurs sexuels dans une liste de blocage empêchant tous ceux y figurant de visiter ou de rejoindre certains sites web, en particulier les sites les plus populaires auprès des jeunes et des adolescents. L'agresseur a naturellement toujours la possibilité de se connecter en utilisant un autre nom ou un faux login, ce qui compromet sérieusement l'efficacité de ces mesures, mais le fait de criminaliser ce type de comportement peut avoir un effet dissuasif.

9. Fournir une assistance long-terme aux victimes. Les enfants et les adolescents ayant fait l'objet d'abus en ligne, par exemple lorsque des images illicites les représentant ont été diffusées sur l'Internet, sont naturellement très préoccupés de savoir qui a pu visionner ces images et quel impact cela aura sur leur vie. Ils peuvent être de fait très vulnérables aux manœuvres d'intimidation et particulièrement exposés à de nouveaux actes d'exploitation et d'abus sexuels. Dans ce contexte, il est particulièrement important de pouvoir fournir des services d'assistance professionnels aux enfants et aux adolescents qui se trouvent dans cette situation. Une telle assistance devra être fournie sur le long terme.

10. Assurer la mise en place et la promotion à large échelle d'un mécanisme permettant le signalement rapide et aisé des contenus illicites ainsi que de tout cybercomportement illégal ou inquiétant, autrement dit d'un système similaire à celui mis en place par la *Virtual Global Taskforce* (www.virtualglobaltaskforce.com). L'utilisation du système i24/7 d'INTERPOL devrait être encouragée.

11. Veiller à ce qu'un nombre suffisant des forces de l'ordre soit convenablement formé à la réalisation d'enquêtes en matière de cybercriminalité et puisse accéder aux installations judiciaires adéquates en vue d'extraire et d'interpréter les données numériques concernées.

12. Investir dans la formation pour familiariser les services de police, les autorités judiciaires et les autorités de poursuite avec les méthodes utilisées par les criminels pour perpétrer leurs crimes sur l'Internet. Il convient également de privilégier l'acquisition et l'entretien des installations nécessaires à l'obtention et à l'interprétation des preuves judiciaires en provenance des équipements numériques. Enfin, il est important d'instaurer une collaboration bilatérale et multilatérale de même que des échanges d'information avec les services de police et les organismes d'enquête des autres pays.

Photo credits: www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

Union internationale des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse
www.itu.int/cop

Imprimé en Suisse
Genève, 2011

Avec le soutien de:

Child Helpline International

unicri
advancing security, serving justice, building peace

International Centre
FOR MISSING & EXPLOITED CHILDREN

CHIS