Lignes directrices à l'usage des professionnels pour la protection de l'enfance en ligne

www.itu.int/cop

Mentions légales

Ce document peut faire l'objet de mises à jour ponctuelles.

Les citations de sources extérieures sont signalées et référencées. L'Union internationale des télécommunications (UIT) ne peut être tenue responsable des contenus issus de sources extérieures, y compris des sites Internet cités.

L'UIT ni ses représentants ne peuvent être tenus responsables de l'usage d'aucune information contenue dans ce document.

Limitation de responsabilité

Les références à des pays, compagnies, produits, initiatives et directives spécifiques n'impliquent en aucune manière que ces derniers sont cautionnés ou favorisés par l'UIT, les auteurs de ce document, ou tout autre auteur ou organisation affilié à l'UIT.

Toute requête concernant la reproduction d'extraits de ce document doit être adressée à: jur@itu.int

© Tous droits réservés, Union internationale des télécommunications (UIT), 2011.

REMERCIEMENTS

Ces lignes directrices ont été préparées par l'UIT en collaboration avec des auteurs travaillant pour des institutions majeures du secteur des TIC. Leur rédaction n'aurait pas été possible sans les efforts, l'enthousiasme et le dévouement de ces auteurs.

L'UIT tient à remercier les rédacteurs suivants pour leur précieuse contribution et pour le temps qu'ils ont consacré à la préparation de ce document (par ordre alphabétique):

- Cristina Bueti et Marco Obiso (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Natasha Jackson et Jenny Jones (GSMA)
- Nerisha Kajee et Rob Borthwick (Vodafone)
- Giacomo Mazzone (UER) pour sa contribution basée sur les documents fournis par Marc Goodchild et Julian Coles (BBC)
- Michael Moran (Interpol)
- Brian Munyao Longwe (AfrISPA)
- Lorenzo Pupillo et Rocco Mammoliti (Telecom Italia)

Les auteurs souhaitent remercier Kristin Kvigne (Interpol) pour la précision de ses relectures et de ses commentaires.

L'UIT souhaite remercier Salma Abbasi de l'eWWG pour son implication dans l'Initiative Protection de l'enfance en ligne.

Des informations et des documents complémentaires à ces lignes directrices, mises à jour régulièrement, sont disponibles à l'adresse suivante: http://www.itu.int/cop/

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

Table des matières

Avant-propos

Synthèse 1

Lignes directrices à l'usage des professionnels 2

Eléments essentiels pour l'ensemble des professionnels des TIC

Eléments essentiels pour les diffuseurs

Eléments essentiels pour les fournisseurs d'accès Internet

Eléments essentiels pour les opérateurs de téléphonie mobile

1. Contexte 6

Pour une collaboration de l'ensemble de l'industrie

2. Catégorisation des contenus et des services 8

Diffuseurs

Etude de cas: *La British Broadcasting Company* **(BBC) — Royaume-Uni** 10

Fournisseurs d'accès Internet

Etude de cas: MySpace et les Six points majeurs de la sécurité pour les réseaux sociaux en ligne 17

Etude de cas: Guide de classification des contenus mobiles — Etats-Unis 19

3. Mécanismes de contrôle des contenus 21

Diffuseurs
Fournisseurs d'accès Internet

Etude de cas: Telecom Italia et la Protection de l'enfance — Italie **26**

Opérateurs de téléphonie mobile
Systèmes de vérification d'âge
Contrôle parental

Etude de cas: Contrôle parental ATT MEdia™ Net — Etats-Unis **31**

Etude de cas: Contrôle parental NTT DoCoMo — Japon **31**

4. Eduquer les consommateurs et communiquer avec eux 32

Diffuseurs
Fournisseurs d'accès Internet
Emploi des Conditions d'utilisation
Opérateurs de téléphonie mobile

Etude de cas: Un code de bonne conduite appliqué aux services SMS spéciaux: *Wireless Application Service Providers' Association* (WASPA) — Afrique du sud **40**

Etude de cas: Les «Conseils malins» de Vodafone aux parents — Royaume-Uni **41**

Etude de cas: Le programme Connaissance des médias de la CBBC — Royaume-Uni **45**

Etude de cas: La série Il était une fois le cyberespace, MDA et Okto, Singapour **45**

Etude de cas: Communiquer avec les consommateurs pour contribuer à la lutte contre les SMS non sollicités ou frauduleux **46**

5. Contenus illégaux 48

Conditions d'utilisation et Directives à l'intention des utilisateurs

Mises en demeure

Etude de cas: Service de notification des abus et mise en demeure — Telecom Italia 50

Organismes et lignes de téléassistance

Collaborations interprofessionnelles

6. Problèmes divers 53

Contenus produits par les utilisateurs: le point de vue des diffuseurs

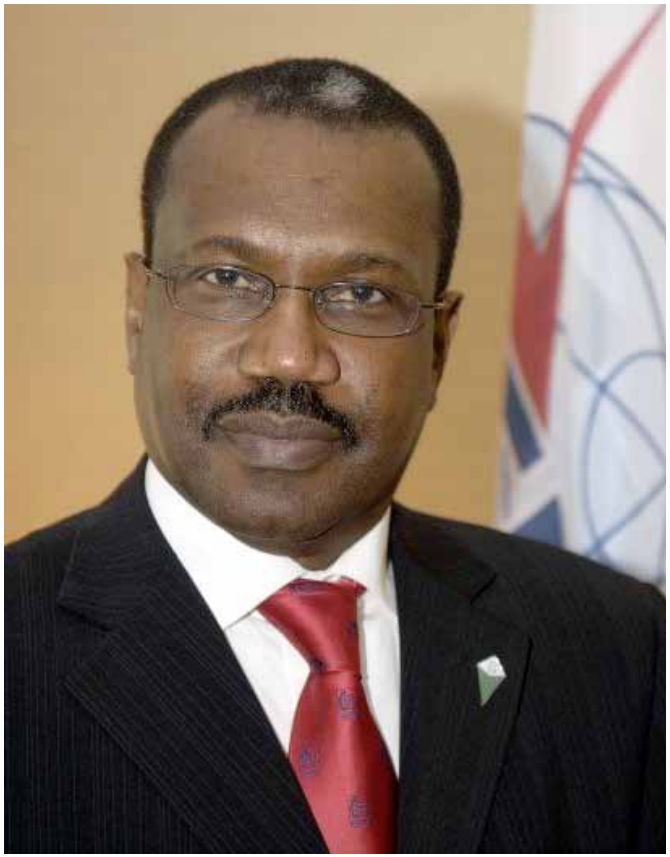
Etude de cas: Comment les diffuseurs peuvent protéger les enfants contre des contenus externes inappropriés: l'exemple de la BBC 55

7. Conclusions 56

8. Informations complémentaires 59

«La protection de l'enfance est un problème qui concerne la planète entière: la solution doit venir de tous»

Avant-propos



Je suis heureux de l'occasion qui m'est donnée de partager avec vous ces lignes directrices, développées grâce à l'aide inestimable de nombreux acteurs du secteur.

La Protection de l'enfance dans le cyberespace, à une époque où l'accès haut-débit à l'Internet est largement disponible, est une question critique, qui exige une réaction coordonnée à l'échelle mondiale. Si les initiatives locales et nationales ont leur place dans cette réponse, l'Internet n'a pas de frontière, et la clé des succès à venir réside dans la coopération internationale.

Tous les acteurs du monde de l'Internet, des diffuseurs aux fournisseurs d'accès et aux opérateurs de téléphonie mobile, sont les acteurs de la victoire contre la cybercriminalité et les cybermenaces, et je suis personnellement reconnaissant de leur soutien.

Hamadoun I. Touré

Secrétaire général de l'Union internationale des télécommunications (UIT)

«La Convention des Nations Unies relative aux droits de l'enfant définit l'enfant comme tout être humain âgé de moins de dix-huit ans. Ces Lignes directrices concernent les problèmes auxquels font face l'ensemble des personnes âgées de moins de dix-huit ans dans le monde. Il est toutefois probable qu'un utilisateur d'Internet de sept ans ait des besoins tout à fait différents de ceux d'un jeune collégien de douze ans, ou d'un internaute de dix-sept ans, déjà presque adulte. Différentes sections de ces lignes directrices présentent des conseils et recommandations adaptés à ces différents contextes. Si la catégorisation en larges groupes peut être utile à un tel guide, il ne faut pas oublier que chaque enfant est unique, et que les besoins spécifiques de chaque enfant exigent une attention particulière et individuelle. De nombreux facteurs juridiques et sociaux peuvent par ailleurs influencer l'interprétation et l'utilisation de ces Lignes directrices en différents endroits du monde.

Il existe aujourd'hui un grand nombre de lois et d'instruments internationaux destinés à soutenir, et souvent à mettre en place, les actions de protection de l'enfance, en général comme dans le domaine particulier de l'Internet. Ces instruments et dispositions légales, dont la Déclaration et le Plan d'Action de Rio adaptés au 3e congrès mondial contre l'exploitation sexuelle des enfants et des adolescents en novembre 2008 proposent une synthèse complète et constituent la base de ces Lignes directrices.»

Synthèse

Ces Lignes directrices ont été préparées dans le cadre de l'initiative Protection de l'enfance en ligne (*Child Online Protection* ou COP[1]), de manière à établir les fondations d'un cyberespace sans danger pour les enfants d'aujourd'hui comme pour les générations à venir.

Les informations présentées dans ce document ont été rassemblées par un l'UIT avec la contribution de professionnels travaillant avec les acteurs majeurs du domaine des TIC: l'association GSM (GSMA), Interpol, Afrispa, l'UER, Telecom Italia, la *Children's Charities Coalition for Internet Safety*, et Vodafone.

La collaboration d'une palette aussi variée de partenaires est significative des changements que suit le secteur de l'Internet, dans le contexte d'une révolution numérique toujours plus rapide.

La convergence est aujourd'hui une réalité acquise dans de nombreux pays, comme le sont les nouveaux défis qui lui sont liés. Aucun secteur particulier du domaine des TIC n'a le monopole du savoir, et la coopération, l'échange d'informations, le partenariat, sont nécessaires à toute avancée.

L'UIT s'associe à tous les auteurs de ce rapport pour appeler les acteurs de l'industrie à promouvoir l'adoption de règles et de normes visant à protéger les enfants dans le cyberespace et à encourager leur utilisation en toute sûreté des contenus en ligne.

Nous espérons que cette collaboration engendrera une société de l'information plus intégratrice, et permettra en outre au Etats Membres de s'acquitter des obligations de protection des droits de l'enfance définies par la Convention relative aux droits de l'enfant adoptée par la Résolution 44/25 du 20 novembre 1989 de l'Assemblée générale des Nations unies, et le Document final du SMSI.

[1] www.itu.int/cop

Lignes directrices à l'usage des professionnels

On trouvera dans cette section un ensemble de conseils pour la protection de l'enfance en ligne. De sorte que soit formulée une stratégie nationale pour la sécurité des enfants dans le cyberespace, il est souhaitable que les acteurs majeurs de l'industrie envisagent l'adoption des stratégies suivantes dans les secteurs indiqués ici:

		Eléments essentiels
Pour l'ensemble des professionnels des TIC		Il est urgent de définir des actions communes, au-delà des seuls organismes de l'UIT agissant individuellement, notamment:
	1.	Le développement de normes et recommandations interopérables pour la protection de l'enfance en ligne, avec pour but de créer une approche globale, communiquée à l'ensemble de l'industrie.
	2.	L'évaluation des possibilités d'une action coordonnée au niveau mondial pour la protection de l'enfance. Une attention particulière doit être donnée à l'élaboration des capacités (tels que les mécanismes de surveillance, de mise en garde, et de notification d'incidents) susceptibles de faciliter la mise en commun des informations.
	3.	L'identification des éléments communs aux différents secteurs de l'industrie (diffusion, Internet, téléphonie mobile) dans le but de développer des chartes de bonne conduite ou de pratiques recommandées qui permettraient aux Etats membres de l'UIT de collaborer plus efficacement avec le secteur privé.
	4.	L'établissement d'accords de coopération entre les gouvernements et le secteur privé, pour le partage de l'information et le développement de capacités spécifiques propres à limiter les risques, tout en encourageant un plus grand usage des TIC par les enfants.

		Eléments essentiels
Pour les diffuseurs	5.	Le développement de règles communes sur les systèmes de notification et de traitement des plaintes. Il s'agit d'éviter les situations où les fonctions de notification externe viennent s'ajouter aux systèmes internes des diffuseurs: ces redondances risquent de compliquer le rapport avec les utilisateurs, et de faire porter à la police et aux autres organismes de surveillance le poids d'un grand nombre de requêtes, que leurs services ne sont pas équipés pour gérer.
	6.	Le développement de normes et recommandations communes, avec pour but de créer une approche globale de la protection de l'enfance en ligne, qui pourra être établie dans l'ensemble de l'industrie.
	7.	L'établissement d'un projet couvrant l'ensemble de l'industrie, visant à la création de procédés d'accord parental plus fiables pour les contenus sensibles, au moins à l'échelle régionale.
		Eléments essentiels
Pour les fournisseurs d'accès Internet (FAI)		Les recommandations qui suivent se proposent de guider les professionnels de l'Internet et les fournisseurs d'accès Internet (FAI) dans le développement d'un cyberespace plus sûr pour les jeunes utilisateurs. Chacun de ces points peut s'inscrire dans une approche plus large de la protection des internautes.
	8.	Les objectifs stratégiques des professionnels de l'Internet en matière de protection de l'enfance dans le cyberespace doivent viser à réduire la fréquence des contenus et des comportements illégaux ou dangereux, et à en limiter l'accès. Les FAI doivent par ailleurs fournir aux parents comme aux enfants les informations et les outils nécessaires à un usage de l'Internet qui en limite les dangers potentiels.
	9.	Sur les sites Internet et les services du Web 2.0, le langage utilisé doit être compréhensible, clair et accessible pour tous les utilisateurs, y compris les enfants, les adolescents, les parents, tuteurs et aidants proches. Cela est particulièrement important pour les Conditions d'utilisation, les politiques sur les données personnelles, les informations relatives à la sécurité en ligne, et les procédures de notification d'abus.
	10.	Sur les notifications d'abus, d'activités illégales et de comportement suspects: il est particulièrement important que les FAI aient en place des procédures fiables et rigoureuses pour le traitement des plaintes. Les plaintes concernant le harcèlement et les contenus ne respectant pas les chartes d'utilisation doivent en particulier faire l'objet d'un traitement prompt, de manière à ce que, le cas échéant, la décision soit prise de supprimer les contenus dangereux. Dans la mesure du possible, les fournisseurs d'accès doivent étudier la possibilité de procédures (telles que des liens permettant de signaler un abus ou un profil d'utilisateur au contenu dangereux pour les mineurs) et doivent pouvoir si nécessaire relayer ces notifications aux autorités.

		Eléments essentiels
	11.	Un «bouton de notification d'abus» peut être présent sur chaque page et chaque service proposé par le FAI. Il permettra de signaler un comportement ou un contenu abusif. Un bouton commun et facile à reconnaître pourrait être conçu, et présent sur chaque écran au même emplacement. Le procédé de notification pourrait être amélioré grâce à l'ajout de moyens techniques destinés aux utilisateurs, qui auraient ainsi la possibilité de joindre à leur notification une capture d'écran, des statistiques de connexion, ou une liste des processus en cours d'exécution. Des informations fournies aux internautes sur les données nécessaires à un traitement efficace des notifications constitueraient aussi un pas important dans cette direction.
	12.	Il serait souhaitable que les fournisseurs d'accès mettent l'accent sur «les comportements acceptables et les comportements à éviter sur le service», dans une langue accessible à tous, dans une mention destinée en particulier aux jeunes internautes et à leurs parents et aidants proches. Il est suggéré qu'une mention de ces informations soit faite en plus de leur inclusion dans les Conditions d'utilisation.
	13.	Nous conseillons aux fournisseurs d'accès de poursuivre l'évaluation de l'efficacité des technologies permettant la vérification de l'âge des visiteurs de leurs services. Il s'agit ici de mettre en place une solution appropriée à chaque service, qui est particulièrement importante pour les services soumis à des restrictions légales sur la base de l'âge des internautes. Ces procédés de vérification d'âge sont souhaitables, dans la mesure où ils sont réalisables dans les cadres juridiques et techniques existants, parce qu'ils fondent des services Internet plus sûrs. La restriction aux personnes majeures de l'accès aux contenus et aux services adultes, comme un accès restreint aux enfants et adolescents pour les sites destinés aux mineurs, sont des solutions possibles.
	14.	Il est conseillé aux fournisseurs d'accès de communiquer activement avec les autorités locales et nationales en signalant tout cas d'abus de mineur aussitôt qu'ils en ont connaissance. Des procédures internes peuvent être mises en place pour s'assurer de la conformité des services à la réglementation en vigueur sur les contenus illégaux, au regard des lois locales et/ou internationales. Il est également souhaitable de procéder aussi régulièrement que possible à l'évaluation des contenus commerciaux hébergés sur les serveurs des fournisseurs d'accès, aussi bien pour les contenus identifiés à une marque que pour les contenus fournis par des prestataires extérieurs. Cela permet de s'assurer qu'aucun contenu illégal n'est accessible par le réseau de ces FAI. Certains outils peuvent aider à cette évaluation, tels que les systèmes de recherche par hachage ou les logiciels de reconnaissance d'images.

		Eléments essentiels
Pour les opérateurs de téléphonie mobile		Les points suivants constituent une «check-list» que les opérateurs de téléphonie mobile sont invités à suivre lors de l'évaluation de leurs procédures de protection des mineurs, que ce soit dans le but d'offrir un environnement mobile plus sûr à leurs jeunes utilisateurs, ou dans la lutte contre l'usage abusif de leurs services pour la distribution ou l'hébergement de contenus à caractère pédopornographique.
	15.	Dans le cas des opérateurs fournissant des contenus qui ne sont pas appropriés pour des publics de tout âge, s'assurer que les contenus font l'objet d'une catégorisation répondant aux attentes nationales en matière de restriction d'âge. Il est aussi nécessaire que ces contenus soient conformes aux normes en cours pour les supports équivalents, et qu'ils soient autant que possible fournis à travers un système de vérification d'âge.
	16.	Si possible, agir en partenariat avec les autres opérateurs du même marché et s'accorder sur des engagements, communs à l'ensemble du secteur, sur une diffusion appropriée des contenus qui ne sont pas appropriés pour des publics de tout âge.
	17.	Offrir des outils permettant aux parents, tuteurs ou aidants proches de contrôler l'accès aux contenus. Ces outils devront eux aussi être établis dans la ligne des attentes nationales pour ce type de support.
	18.	Signaler avec clarté la nature des contenus et des services proposés, de manière à ce que les utilisateurs puissent prendre une décision informée quant à leur consommation et à leurs engagements (par exemple, durée minimale d'abonnement).
	19.	Aider les parents à comprendre l'étendue complète des services de téléphonie mobile que leurs enfants peuvent être amenés à utiliser, de manière à ce qu'ils puissent guider ces derniers dans leur utilisation des services.
	20.	Eduquer les consommateurs sur les moyens mis à leur disposition pour résoudre les sujets d'inquiétude liés à l'utilisation de la téléphonie mobile: spam et messages non sollicités, contacts potentiellement dangereux, etc. Fournir aux consommateurs les moyens de signaler leurs inquiétudes.
	21.	Inclure dans les Conditions d'utilisation une note explicitant la position de votre compagnie sur l'utilisation de ses services pour l'hébergement ou le partage de contenus à caractère sexuel impliquant des mineurs, et son engagement à contribuer à toute enquête concernant des violations des lois en vigueur. Appliquer une règle de suppression des contenus (du type de celle établie aux Etats-Unis sous le nom de *Notice and Take Down* — Mises en demeure) et s'impliquer avec les lignes de téléassistance en place au niveau national, lorsqu'elles existent.

1. Contexte

Le monde numérique que nous connaissons aujourd'hui a radicalement changé la manière dont nous menons nos vies. L'industrie de l'informatique est depuis longtemps numérisée, le secteur des télécoms est maintenant presque entièrement numérique, et le secteur de la diffusion suit un même chemin. C'est aujourd'hui la norme que de pouvoir à tout moment accéder à l'Internet, et plus de temps est consacré à la consommation de produits sur support numérique qu'à tout autre type de support.

La vie quotidienne, de la Chine à l'Italie, déborde de SMS, de courriers électroniques, de rencontres par Internet, de jeux en ligne, de mondes virtuels et de multimédias numériques.

Si ces technologies sont synonymes de confort et de plaisir pour un grand nombre de leurs utilisateurs, les organismes responsables de la régulation, au même titre que les consommateurs, ne s'en trouvent pas moins souvent dépassés par les innovations rapides du secteur.

Avec la multiplication des moyens de distribution, les entreprises, que leur modèle soit traditionnel ou non, font face à de nombreux nouveaux défis.

Pour une collaboration de l'ensemble de l'industrie

Dans notre monde de médias convergents, les distinctions faites traditionnellement entre l'industrie des télécommunications et l'industrie de la téléphonie mobile, entre les compagnies Internet et les diffuseurs, sont de moins en moins pertinentes. La convergence médiatique

rassemble ces courants jusqu'ici distincts en un flot unique, qui touche des milliards d'individus à travers le monde. C'est dans un tel contexte que l'UIT, en collaboration avec l'association GSM, Telecom Italia, l'Union européenne de radiotélévision, la *Children's Charities' Coalition on Internet Safety*, Vodafone et Afrispa, a préparé ces Lignes directrices à l'usage des professionnels pour la protection de l'enfance dans le cyberespace. L'objectif est de proposer un cadre de référence pour que tous les secteurs de l'industrie puissent poursuivre le but commun d'un Internet aussi sûr que possible pour les enfants et les adolescents, par exemple en produisant des codes de conduite ou en créant des sources d'avis et de conseils fiables.

Les fournisseurs d'accès Internet ont accepté depuis longtemps leur responsabilité spécifique quant à la protection de l'enfance en ligne. Les FAI sont en effet à la fois des canaux permettant l'accès à l'Internet, et des réceptacles, à travers les services d'hébergement, de copie cache et de stockage qu'ils fournissent. Il en va de même pour les opérateurs de téléphonie mobile, dont un grand nombre propose maintenant des fonctions allant bien au-delà de leur mission originale de transmission de signaux vocaux et des données. Quant aux diffuseurs, ils sont aussi devenus des acteurs majeurs de l'Internet, en assurant un grand nombre de services en ligne autrefois exclusivement associés aux FAI et aux sociétés d'hébergement. Par la grande visibilité de leurs marques, identifiables et souvent établies bien longtemps avant que l'Internet ne devienne un produit de consommation de masse, les sites

des diffuseurs attirent régulièrement un public très nombreux.

Chacun des secteurs collaborant à ce projet apporte sa propre histoire et ses propres domaines de compétence. Avec ce travail collectif, cette mise en commun de connaissances et d'expériences diverses, l'ensemble de l'industrie se félicite d'être capable de promouvoir plus avant un Internet plus sûr pour tous, mais avant tout pour les enfants et les adolescents.

2. Catégorisation des contenus et des services

L'idée que tous les contenus et tous les services ne sont pas appropriés à tout type de public est bien comprise dans le monde «hors ligne»: films et jeux subissent par exemple une classification correspondant à un âge de consommation, et les programmes télévisés qui présentent un contenu de nature sexuelle ou violente sont assujettis à des horaires spécifiques.

Dans les cas où le contenu en ligne est exactement le même que la version «hors ligne» (par exemple un jeu ou un film pour lequel la seule différence est le canal d'accès), il est possible de reprendre les classifications existantes. Par contre, lorsqu'il s'agit de contenus nouveaux ou modifiés, les fournisseurs de services et de contenus en ligne doivent trouver les moyens de faire connaître aux consommateurs la nature des ces contenus, et la tranche d'âge qu'ils concernent.

Les contenus les plus classiques (les vidéos, par exemple) offrent souvent la possibilité d'une classification établie d'après le cadre existant pour leurs équivalents «hors ligne» dans le pays (ou dans la région, si ces perceptions sont partagées au-delà des frontières). Mais la palette de plus en plus large de nouveaux services interactifs offerts (forums, salons de discussion, sites de réseaux sociaux et services aux contenus produits par les utilisateurs) est plus difficile à classifier dans un sens habituel, et présente des risques potentiels pour les plus jeunes internautes. Ceux-ci peuvent en effet se trouver exposés non seulement à des contenus réservés à un public averti, mais aussi à des comportements inappropriés et dangereux, par

exemple être victimes de harcèlement ou de prédateurs sexuels.

Toutes ces questions sont traitées dans les pages qui suivent. La section consacrée aux diffuseurs traite de la mise à disposition de contenus traditionnels sur un support nouveau. Celle consacrée aux fournisseurs d'accès examine les difficultés que peuvent poser, dans le cadre de la gestion des nouveaux services en ligne, les contenus, contacts et conduites. La section dédiée aux opérateurs de téléphonie mobile examine les approches de différents opérateurs dans le monde, pour les questions de classification et de gestion des contenus et services mobiles.

Diffuseurs

Dans la gestion des contenus inappropriés pour les jeunes spectateurs, les chaînes de télévision bénéficient traditionnellement de la possibilité d'adapter leurs horaires de programmation au public visé. Une émission pour adultes et adolescents sera par exemple diffusée en soirée ou dans la nuit, lorsque les plus jeunes seront au lit.

Avec la diffusion en ligne de plus en plus courante d'émissions accessibles «à la demande», la supervision n'est plus aussi facile pour les parents, et les restrictions d'horaires n'existent plus. Dans ce contexte, les diffuseurs ont tenté de trouver le meilleur moyen de proposer leurs programmes tout en respectant les différents publics.

Les études menées dans ce domaine nous apprennent que les parents préfèrent savoir quel type de contenu (niveau de langue, violence, etc.) peut être problématique, plutôt que de se trouver face à une simple classification.

Certains diffuseurs ont donc développé un système de signalisation: par exemple, le label 'G', appelant à la supervision (Guidance), est apposé par la BBC aux programmes dont le contenu peut être problématique. Une description de la nature du contenu est présentée avec le résumé du programme. La présence du label déclenche le système de contrôle parental par code secret, lorsque l'option est activée.

Note – Sauf mention contraire, le terme de «diffuseur» renvoie spécifiquement dans ce document aux fournisseurs de contenus radiotélévisés classiques, au sens où le «diffuseur» exerce un contrôle éditorial et créatif sur les contenus offerts, que ce soit «sur les ondes» ou en ligne. Ne sont pas concernés par cet usage du terme les prestataires de services permettant la publication de contenus crées par des tiers: ces derniers appartiennent à la catégorie des fournisseurs d'accès Internet.

Etude de cas: la *British Broadcasting Company* (BBC) — Royaume-Uni

L'*iPlayer* proposé par la BBC permet d'accéder aux programmes à la demande, c'est-à-dire sans contrainte horaire, et représente 9% de l'ensemble du trafic Internet au Royaume-Uni. Grâce à ce système, la BBC acquis une expérience certaine de contenus pouvant être problématiques selon l'âge du public.

La version actuelle de l'*iPlayer* de la BBC restreint son installation aux utilisateurs âgés de plus de seize ans. Lors de l'inscription au service, les internautes sont informés de l'existence de la protection par code d'identification, et doivent choisir de l'activer ou non dès cette étape. S'ils choisissent de ne pas activer la protection, des informations leur sont données sur les modalités d'une activation ultérieure.

Lorsqu'un programme n'est pas destiné à tous les publics, il comporte une mise en garde: le signe «G» et une note sur la nature du contenu sont affichés au moment où l'utilisateur choisit de procéder au téléchargement. Au moment du visionnage, le texte apparaît à nouveau, et le code d'identification est demandé, si l'option est activée. Si le code est erroné, un message explique que l'accès au contenu noté «G» n'est pas autorisé.

La BBC proposera bientôt des contenus transmis en flux continu pour son *iPlayer*, qui pourront aussi être signalés par le même «G», et protégés par code d'identification, avant le visionnage. Ces mécanismes pourront être renforcés par l'intégration en un système unique des moyens de téléchargement et de lecture en chargement continu.

Le système et la signalétique de la BBC ont été adoptés par d'autres diffuseurs du Royaume-Uni, tels ITV, *Channel Four* et la chaîne FIVE, pour leur offre à la demande.

La BBC a une stratégie bien définie d'accompagnement des enfants, depuis la petite enfance jusqu'à l'âge adulte: elle propose trois sites dont le niveau de protection est adapté à l'âge de l'utilisateur, à sa compétence informatique, à son indépendance et à sa maturité; elle offre aussi des services éducatifs spécifiques (BBC Learning).

1. Les sites CBeebies (www.bbc.co.uk/cbeebies) et CBBC (www.bbc.co.uk/cbbc) donnent aux enfants et à leurs parents la possibilité d'interagir entre eux et avec le diffuseur, dans un environnement sûr et accessible. En plus de contenus interactifs de qualité destinés aux enfants, ces sites proposent un portail vers les meilleurs services extérieurs pour les moins de douze ans.

2. L'objectif est de responsabiliser les enfants et de leur permettre de créer une relation plus riche avec la BBC, ses personnages et ses produits, ce qui a pour résultat leur plus grande implication et leur impact plus direct sur les sites. Une gamme d'outils interactifs et créatifs est proposée dans ce but à tous les

enfants britanniques. Quelles que soient leur origine et leurs compétences informatiques, ils ont la possibilité de publier leur propre contenu, leurs réflexions et leurs opinions. Un service d'information continu est aussi offert, dans le cadre de *Newsround*, et une section intitulée *PressPack* met à la portée des enfants les sujets qui les intéressent.

3. Pour les adolescents, *BBC Switch* propose des contenus qui encouragent l'interactivité des jeunes gens, sur des sujets qui les concernent. Le site comprend des programmes complémentaires venant de la radio et de la télévision, ainsi que des contenus spécifiques. (www.bbc.co.uk/switch)

4. *BBC Learning* est destiné à renforcer le parcours scolaire des enfants. Les compétences et sujets spécifiques à cette période sont déclinés à travers ces initiatives:

Bitesize — Révision des matières principales pour les cinq-seize ans (www.bbc.co.uk/schools/ks3bitesize).

Blast — développement de la créativité pour les adolescents, centré sur la production artistique, en partenariat avec des organismes artistiques pour la jeunesse (www.bbc.co.uk/blast).

Certains services sont prévus pour être utilisés en classe; d'autres sont utilisés directement par des élèves de plus en plus nombreux, chez eux ou à l'école, sans qu'ils n'aient besoin de tuteurs ou de médiation spécifique.

La BBC travaille en proche collaboration avec l'Ofcom (l'autorité de régulation des télécommunications au Royaume-Uni) et divers diffuseurs et hébergeurs, pour promouvoir les meilleures pratiques de signalisation. La BBC a aussi participé activement à la Commission d'information sur les contenus de l'Association des acteurs large bande (BSG), et est un membre associé de l'Association pour la télévision à la demande (ATVOD), l'organisme d'auto-régulation des services à la demande.

Social Networking

Fournisseurs d'accès Internet

On parle de «contenus produits par les utilisateurs» et de «services du Web 2.0» pour décrire une utilisation d'Internet de plus en plus fréquente, où les utilisateurs créent et distribuent leurs propres contenus écrits ou audiovisuels. Les services du Web 2.0 se déclinent ainsi:

- **Contenu produit par l'utilisateur** — les sites comme les sites Wiki, les blogs et les sites de partages de photos, qui sont conçus spécifiquement pour que les utilisateurs puissent mettre en ligne, partager et consulter des contenus.
- **Les sites de réseaux sociaux** — où les utilisateurs affichent leur «profil» personnel, où l'on trouve des renseignements tels que leur lieu de résidence, leurs goûts et centres d'intérêt (musique, films ou livres), et des photos, des vidéos, des pistes de musique, et des liens vers les profils de leurs amis. On peut aussi y trouver parfois des applications permettant la conversation en ligne, le partage de fichiers, la composition d'un blog, et des groupes de discussion.
- **Les communautés et mondes en ligne** — où les participants choisissent, personnalisent ou créent un personnage appelé un «avatar». Ceux-ci peuvent construire une maison, équiper leur environnement, interagir entre eux, et même échanger de l'argent virtuel dans les transactions entre joueurs.
- **Les jeux en lignes** — où les utilisateurs jouent entre eux dans des mondes complexes, interagissent et discutent.

Il est fréquent que ces catégories se recoupent, et ces sites sociaux occupent une part de plus en plus importante de la culture de la jeunesse: c'est ce que montre une étude indépendante sur l'Internet et les jeux vidéo et leurs risques pour les enfants au Royaume-Uni.

Il peut être utile de distinguer les risques potentiels selon qu'ils sont posés par les «contenus», les types de «contacts», et les «conduites», selon la structure proposée par le Projet Enfants de l'UE en ligne[2]. Le Web 2.0 et sa très grande interactivité autorisent les utilisateurs à communiquer individuellement, à s'adresser à un grand nombre, et à partager en grand nombre. Il est évident que les risques de contacts indésirables en sont d'autant plus présents, ainsi que les risques de conduites illégales. La distinction entre contacts et conduites permet de mieux comprendre les différences, les points communs, et les contre-mesures possibles. «Contact» renvoie à une situation où l'enfant est à la

[2] www.eukidsonline.net/

Note – La section consacrée aux Fournisseurs d'accès Internet propose des approches disponibles pour l'ensemble des professionnels de l'Internet, notamment aux fournisseurs d'accès Internet, et aux fournisseurs de services et contenus électroniques, qui sont désignés dans ce document comme fournisseurs d'accès Internet (FAI). Toutes les recommandations présentes ici ne sont donc pas applicables à tous les FAI.

réception (la «victime») d'un message ou d'une communication; «conduite» renvoie à une situation où l'enfant est à l'origine (l'«auteur») d'un comportement inapproprié[3]. Deux catégories supplémentaires peuvent être ajoutées: le «commerce» renvoie à la possibilité de l'exploitation d'enfants et d'adolescents par des sociétés qui joueraient de leur inexpérience, où aux techniques d'hameçonnage dont les plus jeunes sont des victimes plus faciles. On parle aussi du risque de «dépendance», qui renvoie à la possibilité d'une dépendance maladive à la technologie, qui peut alors nuire à un développement normal.

Du point de vue des professionnels de l'Internet, on peut compter trois objectifs stratégiques majeurs pour la protection de l'enfance en ligne. Ces objectifs appellent à une responsabilisation commune des professionnels et des familles:

- **Réduction de l'offre**: réduire l'offre de contenus, conduites et contacts inappropriés et potentiellement dangereux (professionnels).
- **Restriction de l'accès**: offrir aux enfants et à leurs parents des moyens efficaces pour la gestion de l'accès aux contenus inappropriés (professionnels et familles).
- **Accroissement de la résilience**: aider les enfants à mieux réagir aux contenus qu'ils peuvent rencontrer, leur permettre de trouver une réponse aux contenus et aux contacts inappropriée, et donner aux parents les moyens de les aider, et de faire face aux incidences d'une conduite potentiellement dangereuse et inappropriée de leurs enfants (parents).

A la différence de la radio et de la télévision, l'Internet ne donne pas la possibilité d'un lieu ni d'un moment défini pour l'exercice d'un contrôle éditorial. Celui-ci existe (par exemple avec la modération des contenus produits par les utilisateurs), mais il est largement dispersé au long de la «chaîne de valeur Internet». Cette chaîne comprend les producteurs et agrégateurs de contenus, les FAI, les hébergeurs, les annuaires et moteurs de recherche, les outils de connexion, etc.

A chaque étape de cette filière, un certain nombre d'outils peuvent permettre aux parents de gérer l'accès des enfants à l'Internet (logiciels de contrôle parental, filtrage du contenu pour les moteurs de recherche, sites de vérification d'âge…).

Voyons un exemple de coopération des professionnels de l'Internet avec les familles:

1. Les sites proposant des contenus produits par les utilisateurs retirent de leurs pages les contenus nocifs ou inappropriés.
2. Les enfants et leur famille notifient les sites lorsqu'ils trouvent des contenus inappropriés.
3. Les FAI bloquent l'accès aux contenus illégaux.

[3] *Safer Children in a Digital World: the report of the Byron Review* (http://www.dcsf.gov.uk/byronreview/).

4. Les parents installent des logiciels permettant de filtrer les contenus inappropriés ou potentiellement dangereux.
5. Les sites offrent des conseils clairs et faciles à trouver sur la protection de l'enfance.
6. Les parents parlent avec leurs enfants, et les enfants avec leurs pairs et leurs amis, de la sécurité dans le cyberespace.

Réduction de l'offre:

En prenant les initiatives suivantes, les FAI peuvent atteindre l'objectif de réduction de l'offre de contenus, contacts et conduites inappropriés et potentiellement dangereux:

- Adopter un **système de modération** efficace des contenus produits par les utilisateurs. Par exemple, MySpace passe en revue l'ensemble des messages et des vidéos mis en ligne sur ses services.
- Baser la modération sur les notifications des utilisateurs: une réponse efficace aux notifications émanant de plusieurs utilisateurs, et d'utilisateurs dont l'activité, la réputation et l'ancienneté sont respectées par la communauté, peut permettre de créer une communauté active et «auto-policée» qui agit pour la protection de tous.
- Offrir un système de notification tel qu'il est décrit dans les Conditions d'utilisation ou les Guides d'utilisation: ces systèmes doivent être faciles d'accès et faciles à comprendre à tout âge. Un accusé de réception pour chaque notification, ainsi qu'une réaction rapide, sont souhaitables. Les utilisateurs doivent pouvoir comprendre comment rédiger une notification efficace, et savoir ce qu'il se passe généralement une fois leur message envoyé.
- Relier les notifications à un processus de suppression de contenus: un accord général peut être conclu sur les mesures à prendre et les délais de suppression.
- Eviter les contenus publicitaires inappropriés ou potentiellement dangereux.

Restriction de l'accès:

Cet objectif peut être atteint par les mesures suivantes:

- Des **logiciels de contrôle parental** peuvent permettre aux parents de gérer l'accès de leurs enfants à l'Internet.
- Des **outils pour un Internet plus sûr** peuvent permettre la mise en place de catégories comme les listes blanches, les filtres de contenus, la surveillance de l'utilisation et des contacts, les limites applicables aux horaires et aux programmes accessibles.
- Les **systèmes de contrôle parental** des nouveaux ordinateurs et autres appareils d'accès à l'Internet peuvent être **activés par défaut** à la livraison, avec des messages de sécurité bien visibles expliquant le fonctionnement du système.
- Le **filtrage du contenu**: la plupart des moteurs de recherche proposent une option de filtrage, qui exclut

les images ou les mots clés qui ne seraient pas appropriés pour les enfants.

- L'adoption de **méthodes de vérification d'âge** permet d'empêcher l'accès aux contenus, aux sites et aux services interactifs (comme les salons de discussion) qui présentent des risques de conduites et de contacts inappropriés.
- La **signalisation des contenus**: les fournisseurs de contenus produits par des professionnels (jeux, contenus contrôlés et édités) doivent offrir une signalisation claire décrivant le contenu des sites pour savoir s'il est adapté à un jeune public.
- L'**exclusion totale du réseau** est une option, dont la régulation peut se faire au niveau national, pour les contenus qui sont clairement illégaux, comme la représentation d'abus sur les enfants.

Accroissement de la résilience:

Aider les enfants à gérer les risques et à mieux réagir est un objectif important et complémentaire des objectifs précédents.

Si les parents et leurs enfants jouent un rôle dans la réduction des contenus inappropriés (en notifiant les sites des abus constatés, par exemple), la responsabilité en revient principalement aux professionnels. Et bien que l'industrie joue un rôle pour former la résilience des enfants (en leur proposant des conseils sur la sécurité, par exemple), l'impact le plus important en ce domaine vient très certainement de l'ensemble de l'entourage adulte des enfants.

Les rôles différents des professionnels et des familles mais qui coïncident en partie en ce qui concerne les trois objectifs sont très importants et font ressortir le besoin de stratégies communes, développées au niveau national, qui pourront mettre tous les atouts du côté des familles et des professionnels pour assurer la protection de l'enfance.

Par l'étude des forces et des faiblesses des systèmes de protection mis en place, et l'examen des différentes lois nationales, les professionnels de l'Internet peuvent aboutir à une autorégulation en élaborant un Code de déontologie. Plus transparents que les lignes directrices sur la bonne pratique, si l'organisme qui les coordonne les publie de manière efficace, ces codes peuvent être accompagnés de mécanismes donnant une voix aux parents et aux enfants.

Opérateurs de téléphonie mobile

De plus en plus d'opérateurs de téléphonie mobile offrent un accès à une gamme très riche de services, de jeux, musique, programmes vidéo, etc. Dès lors, ils font face à la question de la gestion de l'accès de leurs clients à des contenus qui seraient soumis à des restrictions d'âge s'ils étaient accessibles par d'autres moyens.

Etude de cas: MySpace et les Six points majeurs de la sécurité pour les réseaux sociaux en ligne

- **Vérification des images et des vidéos**: les sites sont encouragés à passer en revue les images et les vidéos hébergées, pour supprimer celles qui ne sont pas appropriées.
- **Vérification des groupes de discussion**: les sites de réseaux sociaux sont encouragés à vérifier les groupes de discussions, pour y supprimer les sujets dangereux, les propos encourageant à la haine, et les comportements illégaux qu'ils pourraient y trouver.
- **Bannissements des auteurs de crimes sexuels**: les sites sont encouragés à empêcher les auteurs de crimes sexuels de s'inscrire, en utilisant les technologies déjà en place.
- **Des efforts réels et efficaces pour faire appliquer les règles sur l'âge minimal**: les sites doivent faire respecter l'âge minimal en place, et prendre des mesures propres à identifier et exclure les utilisateurs qui ont déformé la vérité pour accéder aux services.
- **Protéger les plus jeunes utilisateurs contre les communications non sollicitées**: par défaut, le système de sécurité des sites doit interdire aux adultes de contacter les enfants de moins de seize ans qui ne les connaissent pas dans le monde physique.
- **Coopération avec les autorités**: tous les sites doivent avoir un accès direct aux forces de l'ordre et aux autorités, pour les enquêtes de routine comme pour les urgences.

La gamme de plus en plus large des services interactifs et des communautés appelle à une nouvelle réflexion sur la protection de l'enfance. De nombreux sites de réseaux sociaux ont par exemple un âge minimal d'utilisation cité dans leur Conditions d'utilisation: les utilisateurs les plus jeunes peuvent être exposés à différents dangers (usurpation d'identité, contacts inappropriés, etc.) s'ils publient trop d'informations les concernant.

De manière à offrir une approche commune et transparente, les opérateurs de téléphonie mobile et les fournisseurs de contenu d'un grand nombre de pays ont décidé de collaborer à un système de classification. Il s'agit généralement de classifier les contenus commerciaux (c'est-à-dire produits par les opérateurs eux-mêmes ou par des tiers avec lesquels ils ont des accords commerciaux), en suivant les normes nationales et les approches suivies par les médias équivalents (jeux et films par exemple).

La classification proposée par d'autres secteurs doit en effet être reprise lorsque c'est possible: par exemple, pour un film, une bande-annonce, un jeu (dans la mesure où les images sont les mêmes dans la version mobile), de manière à ce que les utilisateurs du pays reçoivent et éprouvent le contenu de la même manière sur différentes plateformes.

Compte tenu des difficultés pratiques liées à l'établissement de l'âge de l'utilisateur final de contenus mobiles, un certain nombre de marchés nationaux (comme l'Australie, le Danemark, la Nouvelle-Zélande) ont établi une classification simple, à deux niveaux: contenu pour adultes seulement, et contenu tous publics.

Le code Australien s'est par exemple servi des travaux de la Commission de classification pour aboutir à deux catégories: «accès restreint» (interdit aux moins de 18 ans) et «sans restriction» (tous publics). Aux Etats-Unis, les opérateurs ont créé, sous les auspices de l'Association pour les télécommunications et l'Internet cellulaires (CTIA), une grille qui inclut programmes télévisés, films, musique et jeux dans l'une ou l'autre de leurs catégories — «accès cellulaire» (tous publics) ou «accès restreint» (interdit aux moins de 18 ans). La CTIA en résume ainsi le résultat:

Cette approche binaire permet la vente d'une gamme complète de contenus commerciaux légaux par les opérateurs et par des tiers, tout en respectant les normes nationales. Elle permet de gérer les risques les plus importants, et rend compte du fait que la majorité légale est l'âge le plus facile à vérifier pratiquement (par la présence sur les listes électorales, par exemple, ou par la possession d'une carte de crédit).

Certains marchés ont toutefois fait le choix d'une approche plus précise. L'Allemagne a adopté pour la classification des contenus commerciaux un système en trois catégories, inspiré de la classification de la FSK pour le cinéma en Allemagne:

- Contenus/services «pour tous»: accessibles à tous par défaut.

Etude de cas: Guide de classification des contenus mobiles — Etats-Unis

- Contenus/services classés «16 ans»: accessibles à tous par défaut, avec l'option pour les parents d'interdire l'accès.
- Contenus/services classés «18 ans»: bloqués par défaut pour tous, doivent être débloqués par vérification d'âge.

En France, le système recommandé comprend quatre catégories (tous publics, interdit aux moins de 12, 16 et 18 ans). Il a été crée en consultation avec un grand nombre d'acteurs différents du secteur, sous les auspices du Forum des droits sur l'Internet, et annoncé au public en octobre 2006. Les quatre niveaux différents facilitent la gestion de l'accès aux services interactifs et aux contenus produits par les utilisateurs (dont la plupart ne

Les contenus mobiles seront classés comme «Contenu à accès limité» ou «Contenu à accès général» d'après les critères en place pour la classification des films, des programmes de télévision, de la musique et des jeux.

Les contenus sont «à accès limité» s'ils présentent au moins l'un des traits suivants:

Contenus à accès limité:

- Violence verbale extrême.
- Violence physique extrême.
- Comportements ou activité sexuels explicitement représentés > nudité.
- Propos incitant à la haine.
- Représentation explicite de l'usage de substances illégales.
- Représentation de toute activité interdite par la loi aux personnes de moins de 18 ans, tels que les jeux d'argent.

Tout contenu qui ne fait pas l'objet d'une classification en «accès limité» sera considéré «à accès général» et sera disponible pour tous les consommateurs.

Une description plus détaillée de ce guide peut être consultée à cette adresse http://www.ctia.org/advocacy/index.cfm/AID/10394

posent pas de problème pour les enfants les plus grands, sans être classés «adulte», ni appropriés pour les plus petits.)

Pour accéder aux contenus interdits aux moins de 18 ans, les utilisateurs doivent se soumettre à la procédure de vérification d'âge. Les catégories «12 ans» et «16 ans» correspondent à deux niveaux distincts de contrôle parental:

- Contrôle parental de premier niveau: interdit l'accès aux contenus commerciaux déconseillés aux moins de 16 ans, aux sites hébergeant des contenus produits par les utilisateurs et services interactifs qui encouragent les contacts réels (les sites de rencontres, par exemple), et l'Internet.
- Contrôle parental renforcé: interdit l'accès à tous les contenus déconseillés aux moins de 12 et 16 ans, à tous les services de contenus utilisateurs et interactifs, et à l'Internet.

Les systèmes de classification des contenus sont définis soit par la communauté des opérateurs de téléphonie mobile, soit par un organisme externe qui possède l'expertise requise. Nombre de pays (par exemple le Danemark, la Malaisie, Singapour et la Nouvelle-Zélande) ont simplement inclus la classification dans leur Code déontologique national.

D'autre pays, comme la France, ont compté sur un organisme indépendant pour l'établissement de la classification. Le système en deux catégories en place au Royaume-Uni a été établi par l'Organisme indépendant de classification pour l'industrie mobile (IMCB: http://www.imcb.org.uk/) en 2005. En plus de son rôle de rédaction des critères de classification, cet organisme peut remplir une fonction d'arbitration pour les (très rares) différends sur des contenus ou leur classification.

On peut noter que tous les systèmes de classification ne concernent pas des catégories d'âge: Singapour et la Malaisie utilisent un système binaire défini à partir des normes nationales, classifiant les contenus comme «acceptables» ou «inacceptables», sans qu'il y ait de distinction d'âge.

Les systèmes communs à plusieurs secteurs permettent, parce qu'ils simplifient le processus, une réduction des coûts et une plus grande efficacité pour l'ensemble de l'industrie. Ils augmentent aussi la lisibilité pour les consommateurs, en particulier pour les services extérieurs dont la promotion est faite en dehors du portail de l'opérateur (dans la presse, par exemple). Ils autorisent en outre l'utilisation d'outils facilitant la vérification d'âge, comme les codes adultes de certains services SMS payants.

3. Mécanismes de contrôle des contenus

Les fournisseurs de contenus et services en ligne développent différentes approches pour le contrôle de l'accès aux contenus: systèmes de vérification qui demandent à l'utilisateur de prouver son âge avant d'accéder au contenu, ou contrôles parentaux grâce auxquels les parents peuvent superviser la consommation Internet de leurs enfants.

Diffuseurs

Les diffuseurs proposent une variété de contenus et de services, et certains ne sont pas appropriés pour tous les âges. Pour s'assurer que les plus jeunes n'ont accès qu'aux contenus qui les concernent, diverses techniques sont utilisées:

- Identification unique lors de la connexion — Par exemple, pour les services en lignes de la BBC, les enfants doivent donner leur date de naissance, qui permet de déterminer s'ils sont assez âgés pour accéder au service. Il ne leur est pas possible de changer cette information s'ils s'aperçoivent plus tard que leur âge limite leur accès à certains services.
- Accord parental par courrier électronique — La BBC est en train de tester le contrôle parental par courriel, avec un mécanisme d'inscription

Note 1 – Les mécanismes de lutte contre les contenus illégaux, en particulier les contenus impliquant des violences ou des actes sexuels sur mineurs, seront l'objet du chapitre suivante.

Note 2 – Le chapitre 6 donne de plus amples renseignements sur les diffuseurs et leur relation aux contenus produits par les utilisateurs.

grâce auquel les parents peuvent décider des activités et des informations que les enfants pourront trouver sur les sites de PSB. La BBC est par ailleurs engagée dans un programme de révision des règles à appliquer aux adolescents de moins de 16 ans, pour lesquels la question se pose notamment du niveau d'interaction auquel ils peuvent avoir droit avant l'accord de leurs parents.

- De nombreux diffuseurs du service public, dans l'attente de règles plus précises, adoptent pour l'Internet une approche plus stricte[4] que celle pratiquée sur les ondes. La RAI, par exemple, a pour politique de ne publier en ligne que les contenus classés «programme familiaux», reconnaissables à leur papillon blanc. Les contenus identifiés par un papillon jaune (à regarder sous la supervision d'un adulte) ou rouge (pour adultes uniquement) ne sont pas à ce jour disponibles en ligne.

Fournisseurs d'accès Internet

Il est important que les FAI offrent des moyens de contrôler l'accès à certains types de contenus et de services.

Les lois en vigueur dans de nombreux pays spécifient que certains services et contenus ne doivent pas être accessibles pour les enfants (c'est-à-dire pour les mineurs légaux). Lorsque de tels contenus sont proposés de manière commerciale par les FAI, un système de vérification d'âge et de majorité doit être mis en place. Même lorsque ce n'est pas une exigence légale, il est souvent établi que les enfants et les adolescents ne devraient pas avoir accès à des contenus adultes.

Les FAI peuvent être amenés à établir ou utiliser des systèmes de vérification d'âge, de manière à suivre les contraintes légales.

Il est important que les FAI gardent présente à l'esprit l'idée que les confirmations de l'âge par un simple clic de souris ne sont pas sûres, puisqu'elles sont entièrement basées sur l'honnêteté de l'utilisateur. On ne peut toutefois pas ignorer que les solutions qui exigent une confirmation (en demandant une carte de crédit ou d'autres moyens d'identification) ne peuvent garantir leur infaillibilité. L'un des problèmes majeurs associés à la vérification d'âge sur Internet tient en effet à ce qu'il est impossible de s'assurer que l'utilisateur fournissant des renseignements est bel et bien la personne qui correspond à ces renseignements. Même si un utilisateur saisit des informations personnelles lors d'une inscription sur un site, il est virtuellement impossible de confirmer qu'elles sont véridiques.

[4] On peut noter que la BBC a émis des réserves quant à l'activation d'un «bouton rouge» par les utilisateurs qui se trouveraient face à des contenus inappropriés ou problématiques. La principale objection est qu'un trop grand nombre d'options pourrait amener les utilisateurs à quitter les services de la BBC pour des sites moins surveillés. Il est essentiel que les diffuseurs maintiennent leur réputation d'environnement sans danger, tout en prenant garde à ce que les systèmes de notification ne soient pas déstabilisants.

«L'ensemble de l'industrie s'est engagé pour le développement d'une approche responsable de l'usage des TIC par les enfants»

Par exemple, l'utilisation d'une carte nationale d'identité avec un code personnel associé n'est pas nécessairement un moyen infaillible de vérification d'âge, puisque ce sont des informations souvent accessibles par des tiers (tels que les membres d'une même famille).

De telles approches peuvent aussi aller à l'encontre des droits à la protection des données personnelles de l'utilisateur: une carte d'identité peut ainsi dévoiler des informations au-delà de ce qui est strictement nécessaire à la vérification d'âge.

Les FAI font preuve d'une créativité croissante dans leur gestion des problèmes posés par les contenus inappropriés pour les plus jeunes. Les Conditions d'utilisation de MySpace stipulent que l'âge minimal d'utilisation des services est de 13 ans. Pour remédier aux situations où un utilisateur plus jeune aurait menti sur son âge, MySpace utilise un algorithme de recherche qui traque les termes de vocabulaire fréquents des enfants au dessous de la limite d'âge, de manière à trouver puis supprimer les profils d'utilisateurs trop jeunes. La base de donnée de termes est mise à jour régulièrement, pour prendre en compte les changements de comportement et de lexique.

Un grand nombre de FAI propose aujourd'hui aux parents des moyens de contrôler à quels sites, services et contenus leurs enfants ont accès.

Telecom Italia[5] fait un pas de plus: pour suivre les lois italiennes très strictes sur la protection de mineurs, et pour assurer un suivi général de la sécurité des utilisateurs de ses sites commerciaux, le groupe a lancé un programme de collaboration avec les services de police et le Centre national pour la lutte contre la pédopornographie en ligne (CNCPO)[6], en mettant en place une infrastructure techno-

[5] Loi 38/2006 contre l'exploitation des enfants et la pédopornographie, notamment sur Internet; décret 70/2003 sur la régulation du commerce électronique, exigeant des opérateurs de télécommunication qu'ils fassent des rapports aux autorités compétentes sur la cybercriminalité impliquant le réseau de l'opérateur, et les notifications d'abus sexuels sur enfants; Convention européenne sur la cybercriminalité, signée au Conseil de l'Europe le 23 novembre 2001, ratifiée pour l'Italie sous la loi 48/2008.

[6] http://www.poliziadistato.it/articolo/10232-Centro_nazionale_per_il_contrasto_alla_pedopornografia_sulla_rete

Etude de cas: Telecom Italia et la Protection de l'enfance — Italie

Pour permettre aux enfants et aux adolescents d'utiliser l'Internet sans danger, Telecom Italia a pris plusieurs mesures, décrites sur le portail du groupe[7], pour limiter les contenus qui pourraient menacer l'intégrité physique et mentale des plus jeunes; services et outils de protection sont aussi à la disposition des utilisateurs[8].

L'outil le plus important pour les enfants est le **Bureau magique d'Alice**: un système d'exploitation simplifié fonctionnant sur tout PC. Le logiciel permet aux enfants de profiter de l'ordinateur et des fonctions Internet autorisées dans un cadre sécurisé, éducatif et amusant, où un contrôle précis des parents peut être exercé. Ce service s'adresse aux enfants jusqu'à dix ans.

Il a pour caractéristiques principales:

- La **protection de l'ordinateur** contre une utilisation incorrecte par les enfants (évite les modifications accidentelles de fichiers ou de configuration).
- Une **navigation Internet sans danger**, à partir d'une liste de sites établie par les parents.
- Un **service de courrier électronique** spécifiquement conçu pour les enfants, avec une interface graphique exclusive et un carnet d'adresses défini par les parents.
- **Des jeux en lignes et des utilitaires** pour enfants, amusants, éducatifs et instructifs.
- Une interface générale de **contrôle parental**, permettant aux parents de définir et de surveiller le «jardin protégé» de leurs enfants.

Cet environnement sans danger est d'utilisation très facile pour les enfants, et présente différents thèmes de présentation, un navigateur personnalisable («Mon premier navigateur Internet») où les enfants ne peuvent accéder qu'aux sites approuvés par les parents, et un programme de «Courriel magique» où les messages venant d'adresses inconnues sont placés dans un dossier de «quarantaine» jusqu'à l'approbation éventuelle des parents.

Source: Telecom Italia

logique spécialisée et un système de filtres bloquant les sites signalés par le CNCPO.

De plus, pour lutter contre la diffusion de contenus à caractère pédopornographique et protéger les enfants, Telecom Italia a mis en place un système de notification et d'aide en ligne, grâce auquel les utilisateurs peuvent signaler les contenus illégaux qu'ils pourraient rencontrer. Ces notifications peuvent être faites anonymement en remplissant un formulaire standard, et sont analysées et rapidement transmises au CNCPO qui pourra, en tant que service de police, mener une enquête.

[7] www.telecomitalia.com, Sustainability->Hot Topics-> *Tutela dei minori e Abusi.*

[8] Alice Sécurité Totale et Le Bureau magique d'Alice, http://adsl.alice.it/servizi/index.html

Malgré les constantes améliorations dans ce domaine, les contrôles parentaux ne peuvent pas assurer une sécurité totale; mais lorsqu'ils sont combinés à un enseignement sur les pratiques responsables en ligne (voir plus bas, Eduquer les consommateurs et communiquer avec eux), ils peuvent aider les plus jeunes à vivre un Internet plus sûr.

Opérateurs de téléphonie mobile

Les mécanismes de contrôle d'accès aux contenus inappropriés pour tous les âges se divisent en deux catégories:

- La vérification d'âge
- Les contrôles parentaux

La vérification d'âge

Les outils de vérification disponibles aujourd'hui pour des supports plus classiques ne peuvent être directement transférés vers l'environnement mobile. Il n'est pas possible par exemple de vérifier visuellement au moment de l'achat qu'un consommateur a l'âge requis, comme on peut le faire au guichet d'un cinéma ou dans un magasin. On ne peut pas non plus compter sur la supervision des parents comme les chaînes de télévision peuvent le faire, compte tenu du caractère personnel d'un appareil mobile.

De nombreux opérateurs proposent des solutions à cette question, à travers différents systèmes de vérification d'âge. A ce jour, ceux-ci se concentrent principalement sur la vérification d'âge d'adultes qui souhaitent avoir pleinement accès à l'ensemble des contenus et des services. On peut noter que c'est un point particulièrement important pour les opérateurs qui proposent un contenu commercial soumis à des restrictions légales quant à l'âge des utilisateurs.

Diverses approches tirent profit des options existantes en matière de vérification d'âge, tels que:

- Systèmes de cartes nationales d'identité.
- Cartes de crédit.
- Codes fiscaux.
- Listes électorales.
- Vérification des papiers d'identité en magasin ou par voie postale.
- Contrat ou contact préexistant avec la personne réglant les factures.

Une fois la vérification effectuée, l'opérateur fournit au client un code d'identification qui devra être saisi pour chaque service pour adultes; dans d'autres cas, la vérification donne lieu à la création d'un «profil adulte» sur le compte du client, pour qui l'ensemble des services est débloqué.

Parce qu'il est difficile de contrôler en ligne l'âge d'un utilisateur avant la majorité légale, les opérateurs permettent aux parents de surveiller à quels contenus et services les plus jeunes utilisateurs peuvent accéder.

Les contrôles parentaux

Si les mécanismes de vérification d'âge sont un exemple de mesures proactives de la part des opérateurs, les contrôles parentaux donnent l'initiative aux parents, qui doivent appliquer ces contrôles de la manière qui leur semble appropriée.

De nombreux opérateurs, dans différents pays, ont déjà mis en places des systèmes de contrôle parental: pour certains, les contenus commerciaux adultes sont tout simplement bloqués, pour d'autres cette option fonctionne en combinaison avec des systèmes supplémentaires, comme des restrictions sur les horaires ou les services payants.

La plupart des systèmes proposent un contrôle qui est soit activé, soit désactivé, et qui empêche d'accéder aux contenus et aux services adultes (classifiés par exemple comme réservés au plus de 16 ou 18 ans) lorsqu'il est engagé. On peut noter quelques exceptions, comme en France, où deux niveaux d'accès différents sont en place, ou dans d'autres pays du globe, où plusieurs catégories sont proposées.

La majorité des systèmes de contrôle parental concernent uniquement les contenus commerciaux: c'est le domaine sur lequel l'opérateur a le plus de contrôle et pour lequel il a de fait une plus grande responsabilité. Au Japon, les opérateurs ont un système de liste blanche/liste noire pour les sites Internet, et d'autres marchés fonctionnent avec des systèmes de filtrage. Mais pour la grande majorité des opérateurs, les options de contrôle parental ne comprennent pas encore de filtre Internet.

Un arrangement provisoire choisi par certains opérateurs de téléphonie mobile consiste à bloquer tout accès à l'Internet lorsque le contrôle parental est activé.

Il y a toutefois de fortes chances pour que l'utilisation de plus en plus répandue de la téléphonie mobile pour l'accès à Internet cause une accélération du développement des outils de filtrage.

Bien sûr, puisque la responsabilité du contrôle est très généralement assignée aux parents ou tuteurs, l'efficacité d'une telle proposition dépend de la promotion et de la sensibilisation qui pourront être faites. Les opérateurs doivent aussi s'assurer que les parents sont conscients que le contrôle proposé par les opérateurs ne peut s'appliquer qu'aux contenus offerts par leur propre réseau.

D'autres options sont possibles: l'intégration d'un système de contrôle parental aux écouteurs distribués par leur réseau, ou l'installation de logiciels de contrôle dans les téléphones: les fabricants de téléphones permettraient aux parents de limiter les personnes qui peuvent contacter leurs enfants et que leurs enfants peuvent contacter.

Etude cas: Contrôle parental ATT MEdia ™ Net — Etats-Unis

AT&T propose à ses clients un système de contrôle parental gratuit, qui permet de limiter l'accès des enfants aux contenus adultes, et de contrôler les téléchargements payants (de jeux ou de sonneries par exemple).

Contrôle du contenu: Les parents peuvent choisir d'activer ou de désactiver le Filtre de contenu. S'il est activé, l'accès aux sites adultes (conversations en direct, rencontres) du portail AT&T's MEdia™ Net est interdit, ainsi que l'accès par la fonction de recherche aux contenus Internet externes.

Si le contrôle parental est désactivé, tous les contenus sont accessibles. Par défaut, le contrôle est désactivé.

Contrôle des achats MEdia™ Net: les parents peuvent activer ou désactiver le Bloqueur d'achats. Lorsqu'il est activé, les enfants n'ont pas accès aux contenus payants, tels que les sonneries, les téléchargements, les jeux et les graphismes. Lorsqu'il est désactivé, tous les achats sont possibles. Par défaut, le contrôle est désactivé.

Etude de cas: Contrôle parental NTT DoCoMo — Japon

DoCoMo propose différents niveaux de filtrage des contenus (le filtre i-mode Enfants et le filtre i-mode), en plus d'une option de limitation horaire, qui peut être utilisée seule ou parallèlement aux autres niveaux de filtrage. Les trois options sont offertes gratuitement:

1. Filtre i-mode Enfants: permet d'accéder exclusivement aux sites proposés par le menu i-mode. Les fournisseurs de contenus du menu i-mode sont tenus par contrat à ne proposer aucun contenu potentiellement dangereux: pas de contenu adulte ou pour public averti, pas de violence ni de jeux d'argents, pas de sites de rencontre, de salons de discussion, ni de forums. Le menu i-mode Enfants, qui présente des sites conçus spécialement pour les enfants, est le menu par défaut dans ce mode.
2. Filtre i-mode: permet d'accéder aux sites du menu i-mode, ainsi qu'aux sites externes qui ne présentent pas de contenus potentiellement dangereux.
3. Restriction horaire: interdit l'accès à tout site (i-mode ou externe) entre 22h et 6h.

4. Eduquer les consommateurs et communiquer avec eux

Dans le but de permettre aux utilisateurs de choisir contenus et services en connaissance de cause, et pour aider parents et éducateurs à mieux guider les enfants et les adolescents dans un cyberespace qu'ils veulent sûr, responsable et sans danger, les sociétés de télécommunication et de production de contenus investissent de plus en plus dans des programmes de communication et d'éducation.

Ce chapitre propose différentes approches possibles mises en place par les fournisseurs de contenus et de services en ligne.

Diffuseurs

Les diffuseurs dont les programmes jouissent d'une grande popularité auprès des enfants et des adolescents ont en toute logique un public plus jeune, et de fait une responsabilité plus grande quand à la promotion d'une utilisation sans danger d'Internet.

La position des diffuseurs leur permet en outre d'user de la popularité de leurs contenus pour faire passer des messages simples, lesquels aideront les plus jeunes utilisateurs à se défendre contre les menaces du cyberespace, comme le harcèlement ou les atteintes à la vie privée.

Les diffuseurs peuvent aussi encourager les enfants à demander la permission de leurs parents avant d'utiliser tel ou tel service. Lors de la création d'un compte, un message peut conseiller aux enfants de demander l'accord de leurs parents, et de les avertir de leur utilisation de certains services, comme les forums. Les Conditions d'utilisation peuvent aussi mentionner clairement que les enfants ne peuvent pas utiliser les forums de discussion sans l'accord d'un adulte responsable.

Si un message publié par un enfant suggère que les parents de celui-ci ne savent pas qu'il utilise le service, ou ne veulent pas qu'il l'utilise, le webmestre peut contacter l'utilisateur pour rappeler que l'autorisation de ses parents est obligatoire.

Certains organismes demandent vérification de l'accord parental par courrier électronique, pour plus de sécurité. L'expérience de la BBC nous apprend toutefois que beaucoup d'enfants partagent l'adresse électronique de leurs parents, ce qui retire toute efficacité à ce système; un grand nombre d'utilisateurs de CBBC n'y ont par ailleurs accès que par leurs activités parascolaires, soit parce qu'ils n'en ont pas l'occasion chez eux, soit qu'ils n'y ont pas de connexion Internet.

Une case à cocher, un email de vérification, ne sont donc pas des solutions suffisantes pour s'assurer qu'un adulte responsable supervise en effet les activités de l'enfant en ligne, et ne simplifie par les choses pour les enfants qui se trouvent du mauvais côté de la fracture numérique. L'exploration, à travers l'ensemble du secteur, de nouvelles méthodes d'accord parental où les facteurs sociaux ne sont pas un handicap, et qui peuvent limiter les abus, est encore à faire.

Fournisseurs d'accès Internet

Les professionnels de l'Internet ont la responsabilité d'examiner le rôle et l'importance de la communication avec les utilisateurs, en termes de:

- **Clarté** sur la nature des contenus, les Conditions d'utilisation, et les Chartes d'utilisation.
- **Sensibilisation**, à l'aide de pages dédiées aux dangers de l'Internet, et aux outils disponibles pour la protection de l'enfance.
- **Collaboration**, à travers les formulaires de notification.
- D'**information**, aux parents et aux éducateurs, sur la protection des enfants.
- Et d'**éducation** des enfants pour un Internet sans danger.

Ces points sont repris ci-après en détail.

Clarté *sur la nature des contenus, les Conditions d'utilisation, et les Chartes d'utilisation:*

Les FAI reconnaissent de mieux en mieux l'importance d'une communication claire sur la nature des contenus et des services. Elle permet à tous les utilisateurs, même les plus jeunes, de décider en connaissance de cause de leur consommation.

Pour les professionnels de l'Internet, la clarté, c'est:

- Une signalisation avertissant des contenus qui ne sont pas appropriés pour tous les publics.
- Une communication transparente sur les tarifs, les conditions d'abonnement, les options de résiliations, etc.
- Une définition des Chartes d'utilisation et des Conditions générales d'utilisation.
- Une définition mise à jour des politiques mises place pour répondre aux codes et législation en vigueur quant à la protection des mineurs en ligne.

Sensibilisation, *à l'aide de pages dédiées aux dangers de l'Internet, et aux outils disponibles pour la protection de l'enfance:*

Les FAI peuvent aider à la sensibilisation à ces questions en publiant des informations visibles sur un usage sans danger de l'Internet, et sur les outils proposés sur leur site. Cela permettrait de:

- Promouvoir le dialogue sur les dangers de l'Internet et sur la protection des enfants, et sur les moyens disponibles, comme les options de blocage et les paramètres de confidentialité.
- Partager les conseils de sécurité avec les utilisateurs.
- Présenter une documentation informative et pédagogique.
- Décrire le contexte de la réglementation nationale et internationale.
- Informer l'utilisateur des outils existants pour la protection de l'enfance (contrôle parental, etc.).

Les FAI peuvent aussi participer à la sensibilisation de leurs clients en adoptant un code d'autorégulation, qui correspondra à un ensemble de règles et d'outils pour la protection des mineurs, et en signalant par une marque visible l'adhésion à ce code.

Collaboration, *à travers les formulaires de notification*:

Pour combattre et éviter les contenus dangereux pour les enfants, les FAI peuvent:

- Proposer un espace Internet réservé à la notification des contenus illégaux découverts par les utilisateurs (avec un formulaire qui peut être anonyme);
- Expliquer aux utilisateurs comment signaler tout objet de préoccupation;
- Contacter rapidement les autorités ou services de police concernés, qui pourront enquêter sur les activités signalées. Le personnel du service clientèle des FAI doit être capable de réceptionner et de transférer aux autorités les notifications des utilisateurs.

Information, *des parents et des éducateurs au sujet de la protection des enfants*:

Les fournisseurs d'accès sont conscients de l'importance d'une information claire donnée aux parents et aux enseignants sur l'utilisation des services TIC par les enfants (et sur les problèmes liés, tels que le harcèlement). Une information adéquate permet aussi aux adultes de mieux guider les enfants dans leur utilisation de ces services.

- Les parents et les éducateurs doivent être informés de tous les risques liés à l'Internet, de manière à pouvoir protéger au mieux les enfants. L'information sur ce sujet peut être tournée de manière positive et doit donner aux parents les moyens d'aider à la protection de l'enfance.
- Plusieurs modes de communication peuvent être employés pour transmettre cette information, puisque beaucoup de parents n'utilisent pas l'Internet. Une collaboration avec le réseau scolaire peut être par exemple envisagée, pour offrir aux enfants des leçons sur la sécurité en ligne, et aux parents des conseils sur la supervision. Les FAI doivent aussi promouvoir autant que possible les services de téléassistance permettant aux parents de signaler les cas d'abus sur mineurs.

Les parents et les éducateurs sont invités à:

- S'informer et se former sur l'Internet et les habitudes des enfants en ligne, ainsi que sur la technologie en général;
- Tester et évaluer l'efficacité des moyens technologiques disponibles pour leur famille, et choisir les outils les plus appropriés;
- S'impliquer dans l'usage que font les enfants de l'Internet;
- Etre conscients des risques encourus par les jeunes internautes, de manière à pouvoir les aider dans leur fréquentation du cyberespace;
- Porter une attention particulière aux enfants à risque dans l'entourage de leurs enfants;
- Savoir quand une aide extérieure est nécessaire.

Education *des enfants pour un Internet sans danger*:

Pour les internautes en «culottes courtes», le cyberespace est une mine d'informations et de services utiles et amusants. Mais c'est aussi un lieu où ils peuvent se trouver confrontés à des contenus qui ne leur sont pas destinés.

L'utilisation de l'Internet par les enfants varie selon leur âge et leur développement personnel. Les

plus jeunes sont incapables de comprendre seuls les avantages et les dangers du réseau, et il est donc préférable qu'ils soient en permanence accompagnés d'un adulte (parent ou enseignant) qui puisse les aider et les guider dans leur choix de contenus, et établir les règles à respecter.

Pour ce qui est des adolescents, l'accompagnement est une affaire plus compliquée. Ils sont plus indépendants, et mieux informés de ce que peut offrir l'Internet — et en savent souvent plus que leurs parents et leurs professeurs sur les logiciels en ligne, les messageries instantanées, les salons de discussion, les jeux en ligne, etc. Il n'en est pas moins important que les parents puissent établir des règles, et leur apprendre une attitude responsable, courtoise et vigilante dans le cyberespace.

Il est aussi très important que les FAI informent directement les enfants sur un usage plus sûr de l'Internet. Les enfants doivent apprendre comment reconnaître et signaler les comportements inappropriés. La liste suivante énumère les conseils que les FAI doivent offrir aux plus jeunes utilisateurs:

- «Ne donne jamais d'informations sur l'endroit où tu habites et vas à l'école».
- «N'accepte jamais de rencontrer en personne quelqu'un que tu connais par l'Internet, surtout sans en parler avec un adulte».
- «Ne répond pas aux messages inappropriés (harcèlement, obscénités, insultes) et ne les efface pas – gardes-en une preuve».
- «Si quelque chose ou quelqu'un te met mal à l'aise, parles-en avec un adulte».

- «Ne donne jamais ton code secret, ni ton nom d'utilisateur. Souviens-toi que d'autres utilisateurs peuvent mentir sur les informations qu'ils donnent.»

Les FAI sont aussi encouragés à promouvoir les services de téléassistance auxquels les enfants peuvent s'adresser en cas d'abus sur mineur.

Emploi des Conditions d'utilisation

Il est très important que les FAI et l'ensemble des professionnels de l'Internet placent en évidence les pages réservées aux Conditions générales d'utilisation de leurs services, qui doivent mentionner les mesures prises en cas de manquement. Ces Conditions d'utilisation indiquent généralement que les utilisateurs ne doivent pas

- Télécharger vers le site, publier, transmettre, partager, stocker ou rendre accessible tout contenu dangereux, illégal, diffamatoire, insultant, vulgaire, obscène, frauduleux, raciste, qui constitue une atteinte à la vie privée ou au droit à l'image, ou qui incite à la haine.
- Se faire passer pour une autre personne ou entité, ni donner une idée incorrecte de son âge ou de son affiliation avec toute personne ou entité.
- Télécharger vers le site, publier, transmettre, partager, stocker ou rendre accessible toute information sur la vie privée d'autrui, telle que numéro de téléphone, adresse postale ou électronique, numéros de carte de crédit.
- Chercher à obtenir des informations personnelles d'individus âgés de moins de 18 ans, notamment leur nom, adresse postale ou électronique, ou le nom de leur lieu de scolarisation.
- Télécharger vers le site, publier, transmettre, partager, stocker ou rendre accessible tout contenu comportant des virus informatiques.
- Télécharger vers le site, publier, transmettre, partager, stocker ou rendre accessible tout contenu criminel ou qui informerait sur les moyens de conduire une activité criminelle, qui serait contraire aux droits d'autrui selon toute loi en vigueur dans le territoire ou le pays, ou selon toute loi internationale.
- Participer à tout abus sur des mineurs.
- Harceler, diffamer, escroquer, dégrader tout individu ou groupe d'individus pour quelque raison que ce soit, notamment sur les critères de leur âge, leur sexe, leur handicap, leur origine ethnique, leur religion, ou leur orientation sexuelle.

Une mention des mesures prises en cas de manquement à ces Conditions d'utilisation doit les accompagner, par exemple en ces termes:

- En cas de manquements répétés aux Conditions générales d'utilisation de nos services, (Notre compagnie) applique une politique stricte de suppression des comptes. Elle se réserve le droit de vérifier et retirer les contenus et services produits par les utilisateurs, et de résilier les comptes et supprimer les contenus contrevenants sans préavis.
- (Notre compagnie) se réserve la possibilité d'interdire l'accès à ses sites, et à résilier les abonnements des utilisateurs qui se trouveraient en violation du présent Code de conduite.

Etude de cas: Un code de bonne conduite appliqué aux services SMS spéciaux: *Wireless Application Service Providers' Association* (WASPA) — Afrique du sud

Le code mis en place par la WASPA (Association des fournisseurs de services mobiles) comprend de nombreux engagements à une communication la plus claire possible avec les utilisateurs. Par exemple:

- **La communication et les contenus publicitaires pour tous les services par abonnement doivent faire figurer de manière visible la mention «service par abonnement».**
- **Lorsqu'un utilisateur s'est inscrit à un service par abonnement, un message doit lui être envoyé, avec les informations suivantes:**

a) le prix de l'abonnement et la fréquence des paiements,

b) des informations claires et précises sur les modalités de résiliation,

c) les coordonnées de l'utilisateur.

- **Les membres de services par abonnement doivent recevoir chaque mois un message reprenant les informations a), b) et c).**

L'intégralité du Code de conduite peut être consultée sur le site de la WASPA: http://www.waspa.org.za

Les règles énoncées dans les Conditions d'utilisation peuvent faire l'objet de rappels dans une langue plus proche des utilisateurs, dans le cadre de conseils proposés aux membres de la communauté, et ailleurs dans le site (par exemple sur les pages de téléchargement, pour rappeler aux membres quels types de contenus ne doivent pas être mis en ligne).

Opérateurs de téléphonie mobile

La communication avec les clients, et les efforts fournis pour les former à une meilleure utilisation, aident à s'assurer que les enfants et les adolescents pourront profiter pleinement des services mobiles.

Les opérateurs reconnaissent de plus en plus facilement l'importance d'une communication claire sur la nature des contenus et services inclus dans leur offre: elle permet à tous les utilisateurs, même au plus jeunes, de décider en connaissance de cause de leur consommation. Cette communication nécessite la signalisation des contenus qui ne sont pas appropriés à tous les âges, et des informations claires sur les tarifs, les conditions d'abonnement et de résiliation, etc. Plus les informations sont claires et lisibles, plus les risques seront limités pour les plus jeunes, qui pourraient par exemple s'abonner par erreur à un service alors qu'ils souhaitaient seulement télécharger une sonnerie.

Comme pour tout type de support, les opérateurs de téléphonie mobile ne peuvent endosser seuls l'entière responsabilité d'un usage approprié de leurs services par les enfants et les

Etude de cas: Les «Conseils malins» de Vodafone aux parents — Royaume-Uni

adolescents. Ici comme ailleurs, les parents, aidants proches et éducateurs ont un rôle important à jouer. Dans le cas de la téléphonie mobile, il y a toutefois une difficulté supplémentaire: les adultes sont souvent moins bien renseignés que les enfants sur les fonctionnalités des appareils mobiles. Il est donc particulièrement important de les former.

C'est dans ce but que de nombreux opérateurs investissent dans des programmes éducatifs et des conseils destinés aux parents, et couvrent l'ensemble des questions pertinentes à ce sujet. Par exemple:

- Contenus et services: Expliquer aux parents quels types de services sont aujourd'hui disponibles (Qu'est-ce qu'un réseau social en ligne? Qu'est-ce qu'un service en fonction de l'emplacement? Comment

Vodafone a conçu un livret de «Conseils malins», destiné aux parents. Ce guide propose des recommandations sur divers domaines, comme les salons de discussion, les jeux, les services payants, et le harcèlement.

Les conseils suivants traitent du téléchargement sur les mobiles:

- **Parlez avec vos enfants des services qu'ils utilisent sur leur appareil mobile: ils peuvent par exemple télécharger des sonneries, des fonds d'écran, ou des jeux.**
- **Sachez s'ils partagent les contenus téléchargés avec leurs amis.**
- **Parlez avec vos enfants des contenus que vous n'aimeriez pas qu'ils téléchargent, reçoivent ou partagent avec d'autres.**
- **Insistez sur la nécessité de ne jamais répondre aux messages venant d'étrangers, aux messages bizarres, aux offres de produits très bon marché — elles sont toujours trop belles pour être vraies.**
- **Vérifiez que les téléphones dont le système de contrôle parental est désactivé restent hors de la portée de vos enfants.**
- **Le contrôle parental peut être réactivé en appelant le Service clients Vodafone au 191, en vous rendant dans un magasin Vodafone, ou en ligne à cette adresse: www.vodafone.co.uk**

Le guide «Gardez le contact: la téléphonie mobile expliquée aux parents» peut être téléchargé à cette adresse: http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=VD007645&revisionSelectionMethod=latestReleased&inline=0

est-ce qu'on accède à l'Internet avec un mobile?) et, s'il y a lieu, les options proposées aux parents pour exercer un contrôle.

- Contacts inappropriés: Comment éviter le «danger des inconnus», et que faire si un enfant est harcelé dans le cyberespace ou par SMS.
- Démarche à suivre en cas de vol d'un téléphone, ou si votre enfant reçoit des messages de spam.
- Gérer la confidentialité: Comment ne pas partager d'informations en ligne, garder un profil privé sur les services de réseaux sociaux, etc.

En éduquant les parents, les opérateurs leur donnent les moyens de guider les enfants vers une utilisation plus sûre des services mobiles. Certains opérateurs se sont associés avec d'autres acteurs du marché pour produire et promouvoir des guides pour les parents (par exemple en France[9] et en Irlande[10]). D'autres font la promotion de leurs propres guides auprès de leurs clients.

Il est tout aussi vital d'agir pour faire connaître la disponibilité des outils de contrôle parental, en particulier sur les marchés où ils ne sont pas activés par défaut. Les opérateurs en sont conscients; et communiquent de plus en plus activement sur les options de contrôle: sur les sites Internet, en magasin, avec des lettres jointes aux factures, et en proposant le contrôle parental dès la vente, dans la présentation même du contrat.

Les opérateurs de téléphonie mobile s'adressent aussi directement aux jeunes utilisateurs à travers des programmes d'éducation en ligne et des partenariats avec différentes organisations non gouvernementales présentes sur leur marché. Ils proposent aussi aux enseignants une documentation leur permettant d'informer et d'éduquer les enfants sur le bon usage des services en ligne. «Teach Today» (Enseigner aujourd'hui, www.teachtoday.eu) est un exemple de site créé par un consortium de fournisseurs d'accès mobile et Internet européens.

Parce que l'offre de contenus et de services est toujours plus abondante, les utilisateurs gagneront toujours à recevoir de nouveaux conseils et de nouveaux rappels sur la nature des services, et sur la meilleure manière d'en profiter sans danger. De nombreux opérateurs incluent ainsi des conseils, à l'intérieur même de leurs services (dans les salons de discussion par exemple), en rappelant par exemple de ne pas divulguer d'informations personnelles (voir plus haut «Education des enfants», dans la section consacrée aux FAI, pour d'autres exemples). Un certain nombre d'opérateurs envoient d'ores et déjà des rappels indiquant le lieu où ils se trouvent aux utilisateurs de leurs Services basés sur l'emplacement (LBS, ou *Location-Based Services*): ils leur font ainsi savoir que le service est activé, et leur rappellent comment modifier leur profil et le désactiver.

[9] http://www.sfr.fr/media/pdf/offre-sfr/maj-240107/att00013578/701.09Guideparents2007.pdf
[10] http://www.vodafone.ie/download?id=ICIA_PARENTS_GUIDE.PDF

Etude de cas: Le programme Connaissance des médias de la CBBC — Royaume-Uni

CBBC, la BBC des enfants (ou *Children's BBC*) offre un programme d'apprentissage des médias, présenté par un lapin de dessin animé nommé Dongle, du nom des clés de protection physique de certains logiciels. D'après les études menées, les écoliers réagissent très positivement à ce personnage.

Ce programme comprend un questionnaire interactif, une vidéo, et des liens vers d'autres pages, comme «Le savais tu?». Les contenus proposés traitent de la sécurité en ligne et sur les services mobiles, et sont organisés autour des règles à suivre pour être un utilisateur intelligent (smart):

S = Stay Safe: La sécurité avant tout.

M = Don't Meet Up: Ne pas rencontrer physiquement les inconnus

A = Accepting emails can be dangerous: Accepter des courriels inconnus peut être dangereux

R = Reliable?: Ne pas faire confiance à n'importe qui — certaines personnes mentent

T = Tell: Aller parler avec un adulte de tout ce qui est inconfortable, effrayant ou dérangeant

Toutes les pages de la communauté en ligne ont des liens qui renvoient à cette partie. Ces messages sont répétés par les hébergeurs, lesquels apprécient que soit encouragée une attitude correcte des utilisateurs. Mais il est important de noter que si les règles SMART sont très largement utilisées et bien reconnues par les enfants, on pourra en trouver sur la toile plusieurs versions différentes, ce qui entraine une certaine confusion pour certains enfants.

Etude de cas: La série Il était une fois le cyberespace, MDA et Okto — Singapour

La *Media Development Authority* (http://www.mda.gov.sg/) de Singapour a participé à la création d'une série de six épisodes d'animation, diffusée pendant six semaines par la chaine Okto du groupe MediaCorp. Destinée à promouvoir l'Internet et les nouveaux médias, la série met l'accent sur la prudence en ligne. Cette initiative a été mise en place dans le cadre de la campagne gouvernementale d'éducation sur le bien-être et la sécurité en ligne.

La série vise un public âgé de 10 à 14 ans, et présente de célèbres personnages de contes de fées, qui évoluent dans un cadre contemporain et sont confrontés aux nouveaux médias et à l'Internet.

Par exemple, dans le premier épisode intitulé «Le Petit Chaperon rouge et la messagerie instantanée», le personnage principal trouve un message d'une jeune inconnue qui vit bien loin dans les bois. Le Petit Chaperon rouge discute avec la petite fille, et finit par lui dire qu'il va rendre visite à sa grand-mère, dont il donne même l'adresse. On apprend bientôt que la petite fille n'est autre que le Grand méchant loup.

On peut trouver sur le site de la MDA le résumé des cinq autres épisodes: Blanche-Neige et les Jeux en ligne, Pinocchio fait des rencontres par Internet, Les Trois petits cochons et le Grand méchant virus, La Belle au bois dormant et son téléphone portable (http://www.mda.gov.sg/wms.file/mobj/mobj.1334.Annex.pdf)

Etude de cas: Communiquer avec les consommateurs pour contribuer à la lutte contre les SMS non sollicités ou frauduleux

Tous les clients, même les plus jeunes, sont susceptibles de se trouver face à deux formes de SMS frauduleux, dont on peut facilement éviter les pièges à condition d'être bien informé.

Il est possible d'utiliser un SMS pour inviter un utilisateur à appeler ou contacter par SMS un service payant; ce sont des messages du type «Félicitations! Tu as gagné un prix! Appelle vite le XX XX XX XX XX (qui est un numéro à tarif majoré) pour plus d'informations». Ce type de «micro-escroqueries» vise à soulager les utilisateurs d'une partie du montant de leur forfait ou de leur compte mobile.

Une variante de l'escroquerie par «hameçonnage» s'attaque aux clients de téléphonie mobile pour des tentatives d'usurpation d'identité. Un utilisateur peut par exemple recevoir un SMS ou un message sur sa boite vocale qui semble venir du service des impôts, et qui lui apprend qu'une somme d'argent lui est due. Quand il appelle, l'utilisateur est censé donner ses coordonnées bancaires.

Une campagne d'information menée par les opérateurs peut apprendre aux utilisateurs à reconnaître et à prévenir ce genre d'escroqueries. Par exemple, elle peut leur rappeler les indicatifs des numéros majorés et surtaxés, et les risques qu'ils courent en appelant un numéro inconnu qui commence par cet indicatif. Les opérateurs peuvent encourager la consultation des aides éventuellement en place, qui présentent une liste mise à jour des escroqueries les plus répandues. Le programme SCAMwatch (http://www.scamwatch.gov.au/), proposé par la Commission australienne sur les consommateurs et la compétition, en est un exemple: son but est de «vous aider à reconnaître et signaler les escroqueries, et vous en protéger», et comporte une section consacrée aux «arnaques par téléphone mobile».

La deuxième catégorie importante de comportements abusifs par SMS est celle qui s'appuie sur le système des services par abonnement. Ceux-ci sont parfaitement légitimes pour des transactions répétées, telles que l'utilisation d'un même service d'information chaque semaine. Les abus viennent de fournisseurs de service qui laissent croire à un paiement unique, alors qu'un abonnement est souscrit et que le paiement va être répété automatiquement. Une publicité dans un magazine peut par exemple donner l'impression qu'un service correspond à une charge unique, mais est en réalité un service par abonnement. Ces abonnements doivent être annulés par les consommateurs.

Lorsqu'ils se trouvent confrontés à des comportements abusifs par SMS, les consommateurs doivent pouvoir se plaindre auprès de l'opérateur de leur réseau, et/ou de l'autorité nationale de régulation des services payants — par exemple à l'aide d'un SMS envoyé à un numéro largement communiqué. Les plaintes répétées pourront aider ce secteur à identifier les fournisseurs peu scrupuleux. Il pourra à agir en conséquence, de manière à ce qu'il ne soit plus profitable à personne de se livrer à ce genre d'escroqueries.

Les opérateurs peuvent aider leurs utilisateurs à se protéger contre les offres et messages

abusifs en communicant clairement sur les points suivants:

- Ne répondez pas aux invitations à appeler un numéro surtaxé ou à tarif majoré: les personnes qui vous envoient un SMS pour que vous les rapntpeliez utilisent généralement un numéro normal. Même si vous ne reconnaissez pas le numéro d'un appel entrant, vous pouvez éviter les arnaques en prenant note des indicatifs des numéros à tarif majoré dans votre pays.
- Les organisateurs de concours et de tirages au sort n'envoient pas de messages au hasard pour informer les gagnants: si vous ne reconnaissez pas le concours, c'est très probablement une escroquerie.
- Si vous faites l'achat d'une sonnerie, ou de tout autre service, et vous rendez compte que vous recevez régulièrement des sonneries, vous pouvez être victime d'une escroquerie à l'abonnement. Annulez tous les paiements à venir (en vous référant à l'annonce où vous avez découvert le service) et communiquez une plainte à votre opérateur et à l'autorité nationale de régulation.
- Dans les cas où les opérateurs proposent des systèmes supplémentaires pour la notification des messages non sollicités, ils doivent aussi faire l'objet d'une large promotion. En France, par exemple, les opérateurs de téléphonie mobile ont permis la mise en place d'un code SMS avec lequel les utilisateurs peuvent signaler le spam, et d'un site qui reprend et explique le service: http://www.33700-spam-sms.fr/

5. Contenus illégaux

Des opérateurs de plus de soixante-dix pays, représentant plus de neuf cent millions de consommateurs, adhèrent au Code de pratique GSMA relatif aux spam: les signataires s'engagent à s'assurer «que les procédés autorisés pour gagner l'autorisation (de recevoir des messages de marketing) sont clairs et transparents» et à donner aux consommateurs «des moyens évidents, clairs et efficaces pour choisir de ne plus recevoir de messages de marketing par SMS ou MMS».

La communication est bien sûr une voie à double sens, et un grand nombre d'opérateurs proposent aujourd'hui des moyens de les contacter pour signaler un problème ou un sujet d'inquiétude; leur personnel est formé pour traiter les questions de contact ou de contenu inapproprié, de vol d'appareil ou de spam, et les requêtes concernant l'activation ou la désactivation du contrôle parental.

Comme nous allons le voir, un traitement adapté des notifications émises par les consommateurs constitue une étape majeure de la lutte contre les contenus illégaux, et parfois particulièrement dangereux pour les enfants, dans l'environnement mobile.

Tous les fournisseurs de services Internet, fixes ou mobiles, doivent collaborer avec les autorités et les forces de l'ordre pour remplir leurs obligations au regard de la loi, relativement aux contenus illégaux. Beaucoup de fournisseurs n'en prennent pas moins des mesures supplémentaires et spécifiques pour lutter contre l'utilisation de leurs services pour héberger ou distribuer des contenus illégaux, notamment à caractère pédopornographique.

Ces initiatives sont par exemple:

- Des Conditions générales d'utilisation et des Directives à l'intention des utilisateurs qui interdisent explicitement les activités illégales;
- Des procédures de suppression des contenus, des mises en demeure du type «Notice and Take Down (Mises en demeure)»;
- Une collaboration et un partenariat avec les lignes nationales de téléassistance.

Conditions d'utilisation et Directives à l'intention des utilisateurs

Les fournisseurs d'accès qui proposent des services où les utilisateurs stockent et partagent des contenus (albums photos, réseaux sociaux, etc.) peuvent se servir des Conditions d'utilisation de leur contrat pour énoncer fermement leur position sur l'utilisation du service pour le stockage ou la distribution de contenus illégaux. Ils peuvent ainsi réaffirmer leur collaboration avec le système judiciaire, et se réserver le droit de prendre les actions appropriées, comme de retirer les contenus illégaux, et de bloquer le compte des utilisateurs contrevenants.

On retrouve souvent dans des Directives à l'intention des utilisateurs les mêmes points développés dans les Conditions générales d'utilisation: ces directives proposent, dans un langage plus facile à comprendre et plus proche des consommateurs, les règles de bonne conduite à suivre sur les services. On peut généralement accéder à ces directives depuis le service en question, ou au moment de l'inscription.

Les fournisseurs ont aussi la possibilité d'évaluer et de contrôler régulièrement les contenus hébergés sur leurs serveurs (que ce soit des contenus liés à la marque du fournisseur, ou des contenus hébergés par accord commercial), de manière à s'assurer qu'aucun contenu illégal ou potentiellement dangereux n'est accessible sur leur réseau.

Mises en demeure

Les procédés de mise en demeure et de retrait des contenus, qu'ils soient volontaires ou fassent partie du mécanisme légal, sont un élément majeur de la défense des fournisseurs de service et des opérateurs qui souhaitent se prémunir des contenus illégaux: aussitôt avertis de contenus illégaux, les fournisseurs peuvent s'en remettre au mécanisme en place pour qu'ils soient retirés.

De manière à ce que ces mesures aient une efficacité optimale, il est nécessaire que la nature des contenus illégaux soit clairement définie, et que les forces de l'ordre ou les organismes qui les représentent soient capables de confirmer quels contenus vont à l'encontre des lois en vigueur.

Etude de cas: Service de notification des abus et mise en demeure — Telecom Italia

Conformément aux lois nationales et européennes relatives à la protection de l'enfance, la prévention de la cybercriminalité et la lutte contre la pédopornographie, Telecom Italia a créé des centres de traitement des abus spécialisés dans différents types de clients (particuliers, entreprises, grand clients). Ces centres jouent un rôle d'interface entre les utilisateurs (de Telecom Italia, mais aussi de l'Internet en général) et la société, pour traiter les abus et les usages inappropriés des services.

La spécialisation des opérateurs des centres de notification permet à Telecom Italia de traiter différentes sortes d'activités criminelles sur la toile, et de relayer aux autorités compétentes tous les éléments pertinents, comme la présence de contenus à caractère pédopornographique sur le réseau du groupe.

Deux systèmes de prévention sont en place: un mécanisme de notification et de retrait des contenu (du type Notice and Take Down américain), où soit des utilisateurs, soit la police, signalent au centre de traitement les contenus ou le site qui doivent être mis hors-ligne, et par ailleurs un service de filtrage du réseau, commun à l'ensemble de Telecom Italia, qui filtre les adresses DNS et IP et interdit l'accès aux sites ou aux adresses IP. Les listes des adresses à bloquer sont fournies en Italie par le Centre national pour la lutte contre la pédopornographie en ligne, et sont téléchargées automatiquement chaque jour.

Dans le but de réduire la cybercriminalité sur les services, les opérateurs et les fournisseurs de service peuvent opter pour un Service de notification des abus spécifiques auprès de leur service, une ligne nationale de téléassistance, ou un site spécialisé auxquels ils renvoient. Ils peuvent ainsi être informés de la présence de contenus illégaux par leurs clients, les forces de l'ordre, ou les organismes de téléassistance (voir ci-dessous). Si la notification est issue par un membre de la société civile, les opérateurs et fournisseurs d'accès relayeront l'information aux centres d'assistance nationaux ou aux autorités, pour vérifier l'illégalité du contenu ou entreprendre les poursuites appropriées.

Organismes et lignes de téléassistance

Dès 1995, les professionnels du secteur, les gouvernements et les services de police avaient conscience de l'utilisation de l'Internet, dont la popularité croissait déjà rapidement, pour la publication et l'échange de contenus illégaux, notamment à caractère pédopornographique. Sont évoqués alors les différents moyens de lutte contre ce problème: les lignes de téléassistance sont créées, permettant de notifier de la présence de contenus illégaux.

Le premier numéro d'appel pour les contenus pédopornographiques est mis en place aux Pays-Bas en juin 1996, à l'initiative des professionnels de l'Internet, du gouvernement et de la police. D'autres suivent

en Norvège, en Belgique et au Royaume-Uni.

Depuis, de nombreux pays ont mis en place des lignes de téléassistance, et l'Association internationale des centres de téléassistance Internet (INHOPE) compte aujourd'hui près de trente membres répartis à travers le monde.

Au-delà des approches standard de retrait des contenus, la promotion des lignes de téléassistance donne aux clients et au public en général les moyens de signaler les contenus illégaux qu'ils pourraient découvrir, et constitue une étape importante de la lutte contre ces contenus, notamment ceux à caractère pédopornographique.

Collaborations interprofessionnelles

Un certain nombre d'initiatives de collaboration de l'industrie de l'Internet sont aujourd'hui en place, telles que la Coalition financière contre la pédopornographie, la Technology Coalition, ou l'Alliance des opérateurs mobiles contre les contenus pédophiles. Ces actions rassemblent des acteurs majeurs de chaque industrie, dans le but de partager savoirs et savoir-faire autour de la lutte contre les contenus pédophiles en ligne, par le biais par exemple du blocage des URL qui proposent des contenus illégaux.

6. Problèmes divers

Contenus produits par les utilisateurs: le point de vue des diffuseurs

Cette section résume l'approche que peuvent suivre les diffuseurs en ce qui concerne les contenus produits par les utilisateurs sur leurs services.

De manière à s'assurer qu'aucun contenu illégal n'est publié sur les forums de discussion, il est recommandé que les diffuseurs mettent en place différentes procédures de protection:

a) Filtres automatiques: ces filtres peuvent prévenir l'usage de termes inappropriés (obscénités, injures racistes ou homophobes, etc.) dans les pseudonymes des utilisateurs, et dans les messages, dès le moment de leur publication. Les adresses URL externes et de messagerie électronique peuvent aussi être bloquées.

b) Pré-modération: tous les forums peuvent par exemple être pré-modérés par une équipe de modérateurs spécialisés dans l'encadrement des enfants en ligne, qui vérifient que les messages sont conformes aux règles en usage. Les messages peuvent être lus avant leur publication, et les utilisateurs suspects (comme ceux qui ont besoin d'aide) pourront être repérés.

c) Accueil: en plus des modérateurs, une équipe d'accueil peut être mise en place pour gérer les forums du point de vue du public, et être le premier référent des modérateurs préoccupés par tel ou tel utilisateur.

Toute la modération doit être assurée par une équipe travaillant sur place; une vérification des antécédents de chaque modérateur permet de s'assurer qu'aucune agence n'a signalé à leur sujet d'activité criminelle. Les points suivants peuvent de plus être mis en place:

- Le travail à domicile n'est pas autorisé: il s'agit de s'assurer que personne n'a accès aux coordonnées des enfants.
- La modération doit se faire en équipe, de manière à ce que chaque membre puisse partager ses opinions et ses questions sur les messages et les utilisateurs, et que l'équipe puisse gagner une expérience de groupe des comportements des utilisateurs.
- La modération doit suivre des règles strictes, établies à mesure que l'équipe gagne plus d'expérience.
- Les modérateurs doivent travailler à heures fixes, et les forums ne peuvent être utilisables que durant ces heures. Il y a donc toujours un modérateur de service dès lors que les forums sont ouverts.

C'est là un processus qui demande un investissement considérable en temps et en travail; en outre, plus grande est la popularité du forum, plus le travail de modération exigera de ressources.

La sanction ultime est le blocage des utilisateurs qui persistent à se comporter au mépris des règles établies. Les diffuseurs peuvent toutefois envisager d'établir un système basé sur la confiance et la réputation, qui encourage un bon comportement et permet aux utilisateurs de disséminer par l'exemple la meilleure conduite à avoir en ligne.

Les éléments de la communauté les plus respectés peuvent alors être récompensés pour leur comportement, et les perturbateurs perdront leurs privilèges. Tout contenu soumis par les utilisateurs doit être modéré avant d'être mis en ligne.

Des discussions publiques prémodérées mises en place avec, par exemple, les auteurs ou les présentateurs favoris des utilisateurs, font déjà partie des initiatives qui motivent le public ciblé par les diffuseurs à participer à leur communauté en ligne. Les jeunes gens qui auraient songé à mentir sur leur âge pour s'inscrire à des services pour utilisateurs plus âgés peuvent tout à fait être attirés par de tels événements exclusifs.

Les services en ligne des diffuseurs encouragent de plus en plus les utilisateurs à envoyer des photos et des vidéos en plus de texte. Images et vidéos doivent être vérifiées afin de s'assurer que les contenus sont propres à la publication, et que les enfants ne publient pas d'informations personnelles sur eux-mêmes ou sur d'autres (nom d'école ou de rue, numéro de porte, etc.) qui pourraient les mettre en danger, par exemple en cas d'identification par recoupement.

Dans le cas de vidéos proposées par les enfants, il est conseillé aux diffuseurs d'exiger le numéro de téléphone d'un adulte responsable de l'enfant, qui pourra donner son accord formel pour la publication. En accord avec les pratiques établies pour la télévision, cette précaution est importante pour la protection des enfants, par exemple par rapport à un parent séparé qui n'est pas autorisé à entrer en contact avec lui.

Etude de cas: Comment les diffuseurs peuvent protéger les enfants contre des contenus externes inappropriés: l'exemple de la BBC

Les contenus externes vers lesquels Cbeebies et la CBBC proposent des liens font tous l'objet d'une approbation préalable d'un expert, et figurent sur une «liste verte» dans laquelle le moteur de la BBC peut faire une recherche.

Les recherches exécutées par Cbeebies se limitent au site Cbeebies et aux dossiers créés par des producteurs indépendants qui proposent leurs propres programmes Cbeebies.

Le moteur de recherche CBBC est un outil plus complexe qui permet de trouver les meilleurs contenus de la CBBC et du service d'information Newsround, ainsi que ceux de sites soigneusement sélectionnés de la BBC et de l'ensemble de la toile. Tous les sites doivent être intéressants et pertinents pour un public britannique âgé de 7 à 12 ans, et ne doivent pas:

- **Présenter, promouvoir ou référencer des contenus pornographiques, ou ouvertement sexuels (à moins que ce ne soit dans le cadre d'un programme d'éducation sexuelle destiné à cette tranche d'âge)**
- **Inciter à quelque acte illégal que ce soit**
- **Présenter des discriminations sous quelque forme que ce soit**
- **Promouvoir des mauvaises habitudes d'hygiène ou nutritionnelles**
- **Utiliser un langage inapproprié**
- **Avoir pour seule fonction la vente de produits ou de services**
- **Promouvoir les jeux d'argent**
- **Restreindre son offre aux seuls utilisateurs payants**

La BBC n'autorise de liens vers aucun site de réseaux sociaux depuis CBBC. Si les sites externes comprennent des forums, ils doivent être pré-modérés à tout moment. Il n'est pas possible de présenter de liens vers des salons de discussion en direct depuis les sites pour enfants de la CBBC.

La base de données de recherche de CBBC est constamment vérifiée par des processus automatiques qui balaient l'ensemble des sites listés: des mots clé comme «salon de discussion» ou «forum» sont utilisés pour détecter tout changement. En cas de modification d'un site, ce dernier est signalé à un opérateur qui passe le site en revue et l'exclut si nécessaire de la base de données.

Le site Switch opère avec la même rigueur pour la protection de ses utilisateurs. Si la présence de ce programme sur des sites externes fait partie intégrante de l'offre aux adolescents, en permettant à un public qui ne connaîtrait pas les services de PSB de les découvrir, chaque élément de cette présence est modéré et supervisé. La BBC met en évidence de nombreux liens vers des pages sur la sécurité en ligne, et ne propose jamais de liens vers des salles de discussion en direct depuis Switch.

7. Conclusions

Pour que les FAI et les autres fournisseurs de services en ligne puissent participer efficacement à l'Initiative pour la Protection de l'enfance en ligne, il est crucial qu'ils aient une idée précise de la classification des contenus et des services dans la zone juridique où ils opèrent. Une collaboration avec les diffuseurs locaux peut aider à mieux maîtriser ces questions.

Il est aussi important de savoir comment les lois en vigueur dans le pays ou la région comprennent la «localisation» des contenus et l'«emplacement» de livraison ou réception d'un service.

Chaque pays a la responsabilité de produire son propre appareil législatif applicable aux contenus et services Internet dans leur zone d'application. Plusieurs études montrent malheureusement que les lois sont insuffisantes ou inadéquates dans de nombreux pays, et ne peuvent répondre à tous les problèmes liés à la protection de l'enfance en ligne.

Par ailleurs, les vues diffèrent selon les territoires juridiques. Ces différences peuvent être exploitées, au détriment des enfants. Les criminels et les auteurs de maltraitances à l'égard d'enfants savent quels pays ont les lois les plus souples, les systèmes de surveillance et de réaction les moins développés. Ils se dirigeront naturellement vers ces pays, à moins que des mesures ne soient prises.

Etant données ces différences de structures légales et de politiques d'un pays à l'autre, il est impératif que l'ensemble des professionnels de l'Internet suivent les

lignes directrices d'une meilleure pratique, et adoptent des normes et des codes déontologiques reconnus mondialement qui leurs permettent de s'engager sur le plan social pour assurer la protection de l'enfance en ligne.

Dans de nombreux pays du monde, c'est l'industrie de l'Internet qui prend l'initiative, et adopte volontairement une approche d'autorégulation, montrant ainsi qu'elle s'engage fermement en ce qui concerne l'utilisation des TIC et des communication en ligne par les enfants. Se positionner à la pointe de cet engagement responsable est sans aucun doute dans l'intérêt de l'industrie de l'Internet, non seulement parce que c'est moralement le choix le plus juste, mais aussi parce qu'à long terme, c'est assurer la confiance du public dans le support Internet.

Sans cette confiance, la technologie ne pourra jamais offrir pleinement le potentiel considérable qu'elle promet aujourd'hui — pour le développement personnel des individus, et le développement économique et social de chaque pays.

8. Informations complémentaires

Collaboration à l'échelle de l'industrie

Cadre de référence européen pour un usage plus sûr du téléphone portable par les enfants (*European Framework for Safer Mobile Use by Younger Teenagers and Children)*: http://www.gsmeurope.org/documents/safer_ children.pdf

Liens vers les Code de conduite pour un usage plus sûr de la téléphonie mobile par les opérateurs européens (textes originaux et traduction anglaise): http://www.gsmeurope.org/safer_mobile/national.shtml

Code de conduite GSMA relatif au spam: http://www.gsmworld.com/ our-work/public-policy/protecting-consumers/mobile_spam.htm

Programme pour un Internet plus sûr: Responsabiliser et protéger les enfants en ligne: (*Safer Internet Programme: Empowering and Protecting Children Online*) http://ec.europa.eu/information_society/activities/sip/ index_en.htm

Telecom Italia et la protection de l'enfance: www.telecomitalia.com, *Sustainability->Hot Topics-> Tutela dei minori e Abusi*

Etude sur les tests et le filtrage du programme Internet plus sûr: http://ec.europa.eu/information_society/activities/sip/projects/ targeted/ filtering/sip_bench/index_en.htm

Ministère de l'intérieur britannique: Groupe de travail Internet sur la protection de l'enfance: http://police.homeoffice.gov.uk/operational-policing/ crime-disorder/child-protection-taskforce

Classification des contenus

Commission indépendante pour la classification des contenus et services mobiles (Royaume-Uni): http://.www.imcb.org.uk/

Projet Enfants de l'UE en ligne: http://www.eukidsonline.net/

Rapport de la commission Byron sur la sécurité de l'enfance en ligne: http://www.dcsf.gov.uk/byronreview/

Communication et éducation des consommateurs

Contenus éducatifs à l'usage des enseignants, financés par l'industrie de l'Internet: http://www.teachtoday.eu/

Contenus illégaux

Association internationale des centres de téléassistance Internet: https://www. inhope.org/

Alliance des opérateurs contre les contenus pédophiles

http://www.gsmworld.com/mobilealliance

Coalition financière contre la pédopornographie

http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703

Autorégulation des médias

Tous les services en lignes de la BBC sont soumis aux Directives éditoriales de la BBC (http://www.bbc.co.uk/guidelines/editorialguidelines/edguide)

et aux Directives sur les services en ligne (http://www.bbc.co.uk/guidelines/editorialguidelines/onguide

Rapports nationaux

Royaume-Uni: Safer Children in a Digital World: Informe de la Byron Review, (http://www.dcsf.gov.uk/byronreview/

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:

TELECOM ITALIA

AfrISPA
African Internet Service

EBU·UER

GSMA

CHIS

vodafone