

### LE CENTRE DE RECHERCHE INNOCENTI DE L'UNICEF

Le Centre de recherche Innocenti de l'UNICEF (CRI), situé à Florence, Italie, a été créé en 1988 pour renforcer les capacités de recherche du Fonds des Nations Unies pour l'enfance (UNICEF) et soutenir son engagement en faveur des enfants du monde entier. Le Centre contribue à déterminer et à approfondir les domaines d'activité de l'UNICEF actuels et futurs. Ses principaux objectifs consistent à améliorer la compréhension internationale des questions liées aux droits des enfants et à promouvoir la pleine application de la Convention des Nations Unies relative aux droits de l'enfant tant dans les pays industrialisés que dans les pays en développement ou ceux à revenu intermédiaire.

Le Centre est la plaque tournante de la recherche du Bureau de la recherche de l'UNICEF (OOR) chargé de diriger un programme de recherche stratégique sur l'enfance. Le Bureau a pour objectif de concevoir un cadre intégré pour la gestion de la recherche et des connaissances au sein de l'organisation, afin de soutenir ses programmes et politiques mondiaux. En renforçant les partenariats axés sur la recherche avec des institutions universitaires de premier plan et le développement de réseaux tant au Nord qu'au Sud, le Bureau s'efforce de dégager des ressources supplémentaires et de faire pression pour une politique de réforme favorable aux enfants.

Les publications du Centre sont des contributions à un débat global sur des questions relatives aux droits de l'enfant et comprennent un vaste éventail d'opinions. Il se peut donc que le Centre produise des publications qui ne reflètent pas nécessairement les politiques ou les approches de l'UNICEF sur certains thèmes. Les opinions exprimées sont celles des auteurs et/ou des éditeurs et sont publiées par le Centre afin de stimuler et de faire progresser le dialogue sur les droits de l'enfant.

Le Centre collabore avec l'Istituto degli Innocenti, son institution d'accueil à Florence, dans des domaines de travail choisis. Il est financé essentiellement par le gouvernement italien. Certains projets spécifiques bénéficient également du soutien financier d'autres gouvernements, d'institutions internationales et de sources privées, y compris des comités nationaux de l'UNICEF.

Photo de couverture : © UNICEF/NYHQ2010-3011/Giacomo Pirozzi

Conception et mise en page : BlissDesign.com

© Fonds des Nations Unies pour l'enfance (UNICEF) Mars 2012

ISBN: 978-88-6522-005-4

Toute demande d'autorisation de reproduction ou de traduction des publications du Centre de recherche Innocenti de l'UNICEF doit être adressée au : Service de communication, Centre de recherche Innocenti de l'UNICEF, florence@unicef.org.

Pour accéder à nos publications les plus récentes, veuillez consulter notre site Internet : <www.unicef-irc.org/publications/>.

Merci d'adresser toute correspondance à : Centre de recherche Innocenti de l'UNICEF 12 Piazza SS. Annunziata 50122 Florence, Italie Tél. : (+39) 055 20 330

Fax: (+39) 055 20 330 Fax: (+39) 055 2033 220 florence@unicef.org www.unicef-irc.org



La sécurité des enfants en ligne : défis et stratégies mondiaux

# **TABLE DES MATIÈRES**

Remercien	nentsiii	İ
Avant-prop	oosiv	,
Introductio	onv	,
Première p Abus d'enf	partie fants liés aux technologies de l'information et de la communication	
Na	ture et étendue des abus d'enfants en ligne	
Ac	cès des enfants à Internet	;
lm	plications sociales de la fusion des environnements en ligne et hors ligne4	Ļ
Со	mprendre le risque, la vulnérabilité et le préjudice	,
Pai	rents ou pairs : à qui les enfants demandent-ils de l'aide ?	,
Deuxième partie Construire un environnement protecteur9		
Ins	struments et engagements internationaux10	)
Dé	fis en matière d'application des lois et de protection des enfants12	!
Un	cadre de réponse15	,
Conclusior	า	
Références		,
Acronymes		
Glossaire		

### REMERCIEMENTS

La présente publication, La Sécurité des enfants en ligne : défis et stratégies mondiaux, a été coordonnée par le Bureau de la recherche de l'UNICEF, Innocenti, assisté par un panel international de conseillers et de réviseurs. La recherche a été menée en étroite collaboration et concertation avec Child Exploitation and Online Protection Centre (CEOP), le Centre de protection contre l'exploitation des enfants en ligne au Royaume-Uni. Des remerciements particuliers sont adressés aux bureaux de pays de l'UNICEF suivants qui ont fourni des données, des études de cas et des recommandations précieu ses pour ce rapport : Afrique du Sud, Albanie, Brésil, Croatie, Philippines, Thaïlande et (République bolivarienne du) Venezuela.

Cette étude a été rendue possible grâce à une généreuse contribution du Comité japonais pour l'UNICEF.

#### Recherche

Gerison Lansdown, directrice de recherche; consultante indépendante sur les droits et la participation des enfants

Margaret Akullo, experte en criminologie ; coordinatrice de projet du Project Childhood: Protection Pillar, Office des Nations Unies contre la drogue et le crime, Bangkok

John Carr, conseiller-expert en matière d'utilisation d'Internet et des technologies connexes par les enfants et les jeunes

Mark Hecht, conseiller juridique, Société de l'aide à l'enfance d'Ottawa

Tink Palmer, administratrice générale, Marie Collins Foundation

#### Bureau de la recherche de l'UNICEF, Innocenti

Gordon Alexander, directeur

Jasmina Byrne, spécialiste de la Protection de l'enfant

Andrew Mawson, responsable Protection de l'enfant Susanna Nordh, consultante

Claire Akehurst, assistante administrative

### Support et conseil techniques de l'UNICEF

Karin Heissler, spécialiste de la Protection de l'enfant, Planning and Evidence-Building, UNICEF, New York

Priscillia Hoveyda, consultante, Section de la jeunesse de la Division de la Communication, UNICEF, New York

Ravi Karkara, spécialiste de la participation de l'enfant et de l'adolescent, anciennement à la Division Politiques et pratiques, UNICEF, New York

Ann Linnarsson, spécialiste de la Protection de l'enfant, UNICEF, Port-au-Prince; anciennement chargée de programme, Centre de recherche Innocenti de l'UNICEF

Clara Sommarin, spécialiste de la Protection de l'enfant, UNICEF, New York

### Child Exploitation and Online Protection Centre (CEOP) - Centre de protection contre l'exploitation des enfants en ligne

Graham Ritchie, directeur de la section Missing and Trafficked Children

Gabrielle Shaw, chef du département International Relations

#### Conseillers externes/pairs évaluateurs

Alisdair A. Gillespie, professeur de droit pénal et de justice pénale, Department of Law, De Montfort University, Leicester, Royaume-Uni

David Finkelhor, directeur, Crimes against Children Research Center; co-directeur, Family Research Laboratory, Department of Sociology, University of New Hampshire, États-Unis

Ethel Quayle, COPINE Research, Clinical and Health Psychology, School of Health in Social Science, University of Edinburgh, Royaume-Uni

Julia Davidson, directrice, Research in Criminology and Sociology; co-directrice, Centre for Abuse and Trauma Studies, Kingston University, Londres

Lars Lööf, chef de l'Unité pour l'enfance, Conseil des États de la mer Baltique

Lena Karlsson, directrice de l'Initiative pour la protection de l'enfant Save the Children ; anciennement spécialiste de la Protection de l'enfant, Centre de recherche Innocenti de l'UNICEF

Olga Kolpakova, chef du Département des programmes de prévention, Stellit, Saint-Pétersbourg, Fédération de Russie

Rodrigo Nejm, directeur des programmes de prévention, SaferNet Brasil

Sonia Livingstone, coordinatrice de EU Kids Online; professeur et chef du département Media and Communications, London School of Economics and Political Science

Tiago Tavares Nunes de Oliviera, fondateur et président de SaferNet Brasil

Pia Lang, anciennement chargée politique, Programme Un Internet plus sûr, Commission européenne

#### Éditorial

Christine Dinsmore, éditrice Catherine Rutgers, réviseuse Baishalee Nayak, vérificatrice des faits

### **AVANT-PROPOS**

Au cours des vingt dernières années, Internet est devenu partie intégrante de notre vie. C'est avec enthousiasme que nous avons accueilli son potentiel de communication, de divertissement et de recherche d'informations. Pour de nombreux enfants d'aujourd'hui, Internet, les téléphones portables et les autres technologies constituent une présence constante et familière. Pour eux, la distinction entre « en ligne » et « hors ligne » est de plus en plus ténue et ils se déplacent sans transition d'un environnement à l'autre.

Un nombre croissant d'enfants peut à peine imaginer la vie sans profil de réseautage social; vidéos et photographies partagées en ligne - souvent en temps réel - et jeux en ligne. Les jeunes sont incontestablement à l'avant-garde de l'évolution du changement technologique. Leur entrée dans l'âge adulte en ces temps d'innovation exponentielle a élargi le fossé générationnel qui les sépare de leurs parents, leurs enseignants et des autres personnes qui en ont la garde. Cet écart, s'il va en s'amenuisant dans les pays industrialisés, a tendance à s'agrandir dans les pays à faible revenu où les personnes s'occupant d'enfants ont incontestablement moins de possibilités d'accéder aux technologies de l'information et de la communication. Mais la situation évolue rapidement.

À n'en pas douter, Internet apporte de nombreuses possibilités et avantages aux enfants en termes d'impact sur leur niveau d'instruction et d'inclusion sociale. Toutefois, il les expose aussi à des dangers en dépit de leur âge, de leur situation géographique et d'autres limites qui sont plus nettement démarquées dans le monde réel. Sur Internet, les enfants et les jeunes risquent ainsi de voir des images abusives les mettant en scène, d'être manipulés ou attirés dans des dialogues à connotation sexuelle, voire dans une exploitation perpétrée par des adultes délinquants, d'être victimes d'intimidation ou de harcèlement en ligne.

Sur la base de ce constat, le Centre de recherche Innocenti de l'UNICEF, en partenariat avec le Centre de protection contre l'exploitation des enfants en ligne au Royaume-Uni, a collaboré avec un certain nombre d'acteurs afin de réaliser cette étude et d'analyser le comportement en ligne des enfants, les risques et leur vulnérabilité aux préjudices et d'inventorier les mesures de prévention et de protection existantes pour lutter contre les abus et l'exploitation en ligne. L'étude tire des leçons des pays à revenu élevé et intermédiaire vus à travers le prisme de la dynamique que d'autres pays pourraient avoir à partager dans un avenir proche, compte tenu de la vitesse de l'innovation.

À l'analyse, nous avons appris qu'adopter une approche singulière de la lutte contre ces crimes ne porte pas ses fruits. Il est indispensable qu'un effort collectif soit consenti par les décideurs politiques, les services de l'application des lois, les travailleurs sociaux, les enseignants, les parents et le secteur privé pour protéger les enfants de façon systématique. Nous avons aussi découvert que beaucoup d'enfants connaissent bien la navigation sur Internet et sont en mesure d'éviter les risques. Ils se considèrent parfois comme les protecteurs des plus jeunes et sont eux-mêmes des agents de changement. Les enfants devraient être autorisés à exprimer leur avis sur la façon d'atténuer les risques ; ils devraient être écoutés et autorisés à exploiter en toute sécurité les avantages d'Internet. Toutefois, il ne faut en aucun cas surestimer leur capacité à se protéger. Quoi qu'il en soit, il incombe aux adultes de mettre en place un cadre qui garantisse aux enfants un accès égal et équitable à Internet, allant de pair avec un environnement en ligne plus sûr.

L'accès aux connaissances, à la participation, aux loisirs et aux jeux est un droit fondamental pour tous les enfants, comme le stipule la Convention relative aux droits de l'enfant. Dans les mondes réels et virtuels d'aujourd'hui, il est de notre responsabilité collective d'assurer ces droits à tous les enfants.

Gordon Alexander

C. e Leex S

Directeur

UNICEF Bureau de la recherche Innocenti

### INTRODUCTION

Internet, les téléphones portables et autres médias électroniques fournissent aux enfants et aux jeunes un accès à des informations, des contenus culturels, une communication et des divertissements impossibles à imaginer il y a 20 ans à peine. Toutefois, un grand nombre de ces incontestables avantages s'accompagne de dangers. Internet et les technologies connexes permettent de créer et de distribuer plus aisément des images abusives d'enfants et fournissent aux abuseurs d'importantes nouvelles possibilités d'accéder et d'entrer en contact avec les enfants et les jeunes en ligne. Si les technologies de l'information et de la communication (TIC) n'ont pas, à proprement parler, créé les actes criminels liés à l'abus et à l'exploitation sexuels des enfants, elles ont néanmoins accru l'ampleur et le potentiel de certains des plus anciens et des plus courants d'entre eux.

L'expansion de l'accès à Internet pour tous les enfants et les jeunes, sans discrimination ni exclusion, dans toutes les parties du monde, ainsi que la promotion de la citoyenneté et de la responsabilité numériques doivent faire partie des objectifs prioritaires des décideurs politiques soucieux d'accroître les possibilités offertes aux enfants1. La construction d'un accès plus sûr à Internet fait partie intégrante de ce projet. Des questions comme « quelle est la nature du risque à l'échelle mondiale ? » et « quelles sont les stratégies les plus efficaces pour l'aborder? » sont, par conséquent, essentielles. Le but du présent rapport, rédigé par le Centre de recherche Innocenti de l'UNICEF (CRI) en partenariat avec le Centre de protection contre l'exploitation des enfants en ligne (CEOP), consiste à passer en revue les données factuelles disponibles. Dans un premier temps, l'étude s'est penchée sur deux problèmes : la maltraitance sexuelle d'enfants enregistrée en images et la manipulation des jeunes à des fins sexuelles. Une troisième question, le harcèlement en ligne, que de nombreuses recherches s'accordent à qualifier de très important pour les enfants, est également évoqué dans ce rapport.

Des lacunes importantes subsistent dans les connaissances relatives aux défis soulevés par Internet en matière de protection, en particulier dans les parties du monde où sa pénétration a été jusqu'à présent plus limitée. Un travail considérable a été entrepris pour analyser le comportement en ligne des enfants et des investissements ont été consentis afin de mettre en œuvre des stratégies qui ciblent et préviennent la maltraitance dans

plusieurs parties d'Asie, dans toute l'Europe et aux États-Unis d'Amérique. Par contre, la question de la maltraitance et de l'exploitation en ligne des enfants a été nettement moins explorée dans de nombreux pays à revenu faible ou intermédiaire, où l'examen de l'état des connaissances et/ou de la capacité de réponse des organes chargés de la protection des enfants et de l'application des lois laisse à désirer. La recherche sur l'usage d'Internet par les enfants et les jeunes en Afrique, dans une grande partie de l'Asie et de l'Amérique latine (et son incidence potentielle sur le risque) est très limitée. De plus, les conclusions des recherches menées dans différentes parties du monde industrialisé sont parfois contradictoires.

Il serait erroné de croire que la maltraitance des enfants dans laquelle les TIC jouent un rôle n'est un problème que pour les sociétés ou les groupes sociaux plus aisés. L'accès à la toile s'étend rapidement, supporté par la pénétration accrue des téléphones portables et du haut débit. En effet, l'émergence du haut débit a contribué de façon décisive à faciliter la maltraitance des enfants en ligne parce qu'il permet l'échange de fichiers plus volumineux, en particulier ceux qui contiennent des photos, des vidéos et des données audio. Le haut débit commençant à être disponible dans les pays à revenu plus faible, il est plus que probable que si aucune mesure préventive n'est adoptée, les modèles de comportements abusifs constatés ailleurs s'installeront également dans ces pays.

En général, les enfants et les jeunes ont tendance à être des utilisateurs précoces et des innovateurs zélés sur Internet et ils sont souvent bien en avance sur leurs parents ou d'autres adultes en termes d'utilisation, de compétences et de compréhension. Internet, en particulier les réseaux sociaux et autres médias interactifs, fournit de nouvelles formes d'espace social à l'échelle mondiale qui n'existaient pas lorsque la plupart des parents contemporains étaient eux-mêmes des enfants. Les jeunes de toutes les sociétés sont aujourd'hui des pionniers et leurs modes d'utilisation des espaces en ligne défient souvent l'entendement des adultes. Ces espaces peuvent être immensément créatifs mais sont également susceptibles d'exposer les enfants à des dangers que les adultes ne perçoivent, la plupart du temps, que très faiblement.

La facilité d'interaction avec les enfants et entre ceux-ci, le risque de maltraitance sexuelle, les nouvelles technologies en évolution permanente, ainsi que le manque d'intérêt et de compréhension dont témoignent les adultes à l'égard d'Internet ou de l'utilisation qu'en font les enfants, font naître l'anxiété sociétale – ainsi que le sensationnalisme, l'affabulation et les réponses politiques impulsives. Les nouvelles technologies suscitent généralement des craintes quant à leurs dangers potentiels ne reposant souvent sur aucun fondement solide ni sur aucune donnée factuelle. Jusqu'à présent, la crainte populaire voulant qu'Internet présente un danger pour tous les enfants n'a été étayée par aucune recherche². Toutefois, de véritables risques y sont associés et l'étalonnage des mesures de protection appropriées nécessite des informations fiables permettant d'identifier précisément la nature et l'ampleur du risque et des dommages.

Si une grande partie de la recherche et du travail initiaux qui ont mené au développement d'Internet impliquait des acteurs issus des secteurs public et privé, depuis le milieu des années 1990 on considère qu'Internet est détenu et exploité intégralement par des entités du secteur privé. Entre-temps, il est devenu essentiel pour l'économie mondiale et, par extension, pour le fonctionnement efficace d'un grand nombre, toujours croissant, d'économies nationales. Il sous-tend l'infrastructure publique qui assure le fonctionnement optimal des transports, du pouvoir, des banques et d'autres systèmes vitaux. Il joue un rôle majeur dans la vie sociale et politique d'un nombre important et grandissant de citoyens dans le monde entier. C'est précisément à cause de sa dimension que les gouvernements, les institutions intergouvernementales et les autres organes publics ont généralement fait preuve de circonspection lors de la discussion de nouvelles lois ou de nouveaux règlements sur le fonctionnement d'Internet ou sur les attentes placées sur la myriade de grandes et petites entreprises qui constituent l'industrie moderne d'Internet. Néanmoins, la volonté de légiférer et de réglementer Internet est manifestement présente, comme l'ont démontré les réactions des politiques à des phénomènes comme l'utilisation des sites de réseautage social lors de périodes de troubles civils.

Les gouvernements ont tendance à s'attaquer à l'exploitation et à la maltraitance sexuelle en ligne en mettant l'accent sur la construction d'une « architecture » visant à protéger ou sauver les enfants - en instaurant une législation, en poursuivant et sanctionnant les abuseurs, en menant des campagnes de sensibilisation, en réduisant l'accès au risque et en soutenant les enfants victimes de maltraitance ou d'exploitation. Ce sont là des composantes essentielles de toute mesure de protection. À l'échelle internationale, cependant, le progrès est fragmentaire. Ainsi, de nombreux systèmes juridiques ne parviennent pas à adopter une législation efficace pour lutter contre les images abusives d'enfants ou des lois pénalisant le harcèlement. Ajoutons que les parents et les agences chargées de la protection des enfants méconnaissent parfois la nature réelle des dangers ou les stratégies efficaces de protection

ou que ces sujets suscitent chez eux un malaise. La prise de conscience de la maltraitance et de l'exploitation des enfants en ligne ne semble pas être organiquement inscrite dans la grande majorité des systèmes et des mesures de protection de l'enfant. L'intégration de la sensibilisation à la maltraitance et à l'exploitation en ligne dans le programme plus général de protection de l'enfant doit devenir une priorité des décideurs politiques.

La place centrale occupée par le secteur privé sur Internet lui confère des responsabilités majeures en matière de protection des enfants en ligne. En vertu de la définition contemporaine des responsabilités des entreprises en matière de respect des droits de l'homme, récemment formulée à l'échelle internationale dans les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, les entreprises ont l'obligation tant de respecter les droits de l'homme que de prévenir ou de remédier aux incidences négatives sur les droits de l'homme directement liées à leurs opérations, leurs produits et leurs services<sup>3</sup>.Or, la maltraitance et l'exploitation des enfants ont manifestement des « incidences négatives sur les droits de l'homme ». L'industrie a le pouvoir de développer et d'introduire de nouveaux outils pour rendre Internet plus sûr pour les enfants. L'importance de l'action du secteur privé pour soutenir l'application des lois et la sécurité sur Internet est abordée plus loin dans le présent rapport.

L'industrie est confrontée à de véritables défis et craintes. Certaines des mesures susceptibles de contribuer à rendre Internet plus sûr pour les enfants semblent remettre en question le modèle d'entreprises en vigueur actuellement ; elles peuvent sembler restreindre la compétitivité de certaines sociétés ou menacer d'autres libertés inhérentes au fonctionnement actuel d'Internet. Pourtant, il ne fait aucun doute qu'il est dans l'intérêt à long terme d'Internet lui-même – et en particulier des grandes sociétés qui le dominent – que les gouvernements sentent que les préoccupations légitimes concernant leurs citoyens et, en particulier, les enfants et les jeunes, sont prises au sérieux et débouchent sans délai sur des actions. À défaut, on court le risque que les gouvernements ou les administrations régionales se mettent à réglementer et légiférer de façon à affecter négativement Internet en tant que système mondial unique, garant de la liberté d'information.

Étant donné que la recherche sur l'usage d'Internet et le risque qui y est associé a essentiellement été menée au sein du monde industriel, l'extrapolation des conclusions à d'autres contextes socioéconomiques et culturels ne peut se faire qu'avec circonspection. Néanmoins, la recherche menée dans les pays à revenus faible et intermédiaire est suffisante pour suggérer des modèles et des problèmes potentiels. L'une des découvertes importantes réalisées à la fois dans les pays

industrialisés et dans les pays à faible revenu est l'importance de l'action, de l'innovation, de l'exploration et de la découverte par les adolescents sur Internet ; en d'autres termes, la capacité d'agir des enfants est importante lorsqu'ils accèdent aux atouts créatifs d'Internet, lorsqu'ils sont exposés à certaines formes de risque et lorsqu'ils doivent gérer ce risque.

Les mesures de protection doivent trouver un juste milieu entre le droit à la protection contre toute forme de violence, de maltraitance et d'exploitation sexuelles et les droits à l'information, à la liberté d'expression et d'association, à la vie privée et à la non-discrimination tels que les définit la Convention relative aux droits de l'enfant et d'autres normes internationales pertinentes. Cet équilibre doit s'ancrer, prioritairement, dans les meilleurs intérêts des enfants, dans leur droit à être entendu et pris au sérieux et dans la reconnaissance du développement des capacités des enfants et des jeunes. Il est sans doute impossible d'éliminer tous les risques auxquels sont exposés les enfants et les jeunes dans l'environnement en ligne. De plus, au-delà d'un certain point, cette tentative pourrait menacer l'essence même d'Internet et ses multiples avantages.

Il serait totalement erroné de penser que tous les enfants et les jeunes ont les mêmes capacités ou la même aisance face à l'environnement en ligne, ou encore qu'ils disposent des mêmes informations en la matière4. L'utilisation d'Internet par les enfants, ainsi que leur comportement et leur vulnérabilité en ligne diffèrent en fonction de leur âge. Pour être efficaces, les stratégies de protection doivent inclure des mesures et des messages adaptés aux différents âges et niveaux de compréhension. Il est à noter par ailleurs que, dans de nombreux cas, les enfants et les jeunes ont la connaissance la plus pointue de leur propre utilisation des TIC. Le présent rapport soutient que les stratégies de protection efficaces nécessitent, à la fois dans leur conception et leur mise en œuvre, la participation des enfants, en particulier des adolescents, et l'amélioration des capacités des parents et des autres adultes qui travaillent étroitement avec les jeunes, comme les enseignants, afin qu'ils soient en mesure de soutenir et de comprendre l'utilisation par les enfants des TIC et de reconnaître les risques et les dangers qu'ils sont susceptibles de rencontrer. Il s'agit à la fois d'une reconnaissance pragmatique de la réalité et d'une position fondée sur les principes des droits de l'homme.

Le présent rapport évoque la nature et l'importance des abus et de l'exploitation sexuels des enfants et des jeunes en ligne, ainsi que les types de délits perpétrés contre eux. Il tient compte du fossé

générationnel entre les parents et les enfants qui influencent leurs différentes connaissances et implication dans l'environnement en ligne, ainsi que leurs différentes expériences et approches d'Internet et de son utilisation. Le rapport décrit comment les enfants et les jeunes à travers le monde utilisent Internet et s'intéresse de près aux activités et aux expériences spécifiques susceptibles de présenter un risque. Il cible en particulier les activités impliquant une interaction en ligne et hors ligne et analyse les conclusions des recherches identifiant à qui les enfants demandent de l'aide quand les choses tournent mal.

Le défi pour les décideurs politiques consiste à ne pas se perdre en accusations contre le média luimême, mais, au contraire, à coordonner les activités de toute une série d'acteurs publics et privés portant sur une multitude de questions interdépendantes qui, en définitive, ont pour objectif de « construire un Internet plus sûr ». Il s'agit, entre autres, d'intégrer la compréhension des abus et de l'exploitation sexuels des enfants dans la construction de l'accès à Internet, de comprendre l'utilisation des TIC par les enfants et d'élaborer avec les jeunes des stratégies de sécurité efficaces, d'intégrer la prise de conscience et la compréhension de la maltraitance et de l'exploitation des enfants en ligne dans les systèmes de protection de l'enfant, d'assurer l'application efficace des lois contre la maltraitance et l'exploitation en ligne des enfants et d'intégrer la protection de l'enfant dans l'application efficace de la loi. Si l'utilisation d'Internet est moins omniprésente dans les pays à revenu faible et intermédiaire, la protection est un défi auquel ces derniers seront confrontés dans un avenir très proche et qu'ils doivent relever dès à présent.

Le rapport s'intéresse également aux manières d'élaborer un environnement plus sûr pour les enfants et les jeunes pour qui Internet constitue un moyen social de base dans lequel se rejoignent les mondes en ligne et hors ligne. Le rapport cartographie les lois internationales pertinentes, ainsi que les défis clés à relever par les gouvernements et les services de l'application des lois compétents afin d'accroître la protection des enfants et des jeunes. Il soutient qu'une approche à plusieurs niveaux s'impose pour faire face aux menaces potentielles contre le bien-être des enfants et leur sécurité dans l'environnement en ligne. Il conclut ainsi en proposant un cadre de protection stratégique qui poursuit quatre objectifs principaux : 1) autonomiser les enfants et renforcer leur résilience, 2) mettre fin à l'impunité des abuseurs ; 3) réduire la disponibilité des contenus préjudiciables sur Internet et l'accès aux dangers et 4) favoriser le rétablissement et la réadaptation des enfants ayant subi un préjudice.



# PREMIÈRE PARTIE

## ABUS D'ENFANTS LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

# Nature et étendue des abus d'enfants en ligne

Une étude menée par Sonia Livingstone et Leslie Haddon pour EU Kids Online a recensé une série de catégories permettant de comprendre les risques et les préjudices liés aux activités en ligne. Ces catégories font toute la lumière sur les caractéristiques des comportements en cause et contribuent à orienter les chercheurs et les politiques vers leurs différentes implications : a) préjudice dû à des contenus en ligne inappropriés (l'enfant est le destinataire passif de contenus nuisibles à caractère pornographique ou sexuel); b) préjudice de contact (l'enfant étant sollicité par un adulte ou un autre enfant pour participer à des activités, dont les abus sexuels, qui sont ensuite photographiés et publiés, il devient la proie d'une manipulation en ligne à des fins sexuelles ou d'un harcèlement) et c) préjudice comportemental (l'enfant adopte un comportement risqué ou abusif, par exemple en créant ou en téléchargeant du matériel pornographique, en rencontrant physiquement un adulte qu'il a connu en ligne, en mettant en ligne des images de luimême ou d'un autre jeune, en téléchargeant des images abusives d'enfants ou en pratiquant le harcèlement)<sup>5</sup>. La panoplie de comportements d'adultes impliquant des abus sexuels commis sur des enfants en ligne inclut l'exploitation sexuelle par des adultes de leurs propres enfants ou de ceux des autres afin de produire des images d'abus d'enfants; le téléchargement de ces images à des fins personnelles ; la création et la distribution d'images et la tentative de prendre contact en ligne avec des enfants afin de les exploiter.

On estime à plusieurs millions le nombre d'images de maltraitance d'enfants circulant sur Internet et à plusieurs dizaines de milliers le nombre d'enfants y apparaissant<sup>6</sup>. L'une des différences importantes entre les images en ligne et hors ligne est le fait qu'une fois en ligne, une image peut circuler indéfiniment et qu'il est pratiquement impossible de limiter le nombre de fois ou de personnes qui la voient ou la transfèrent. Certaines images disponibles aujourd'hui pourraient

avoir été produites il y a plus de 20 ou 30 ans et trouvent vraisemblablement leur origine dans des photographies tirées de films ou de vidéos numérisés depuis lors<sup>7</sup>. Toutefois, la majorité des images circulant dans le cyberespace sont bien plus récentes et sont liées à l'émergence de caméras numériques bon marché, faciles à utiliser, et au développement d'Internet.

La majorité des enfants apparaissant dans les images d'abus d'enfants actuellement en ligne sont des filles caucasiennes pré-pubères (âgées de moins d'un an à 10 ans)8. Cette prépondérance reflète peutêtre le fait que jusqu'ici les recherches ont pour la plupart été menées dans les pays occidentaux et que les délinquants préfèrent les enfants partageant leurs propres caractéristiques ethniques. Elle peut également s'expliquer par la plus grande disponibilité des TIC et d'autres technologies permettant de capturer et de distribuer des images dans les pays industrialisés. On constate à la fois une tendance claire à la baisse de l'âge des enfants et une propension des images à devenir plus graphiques et violentes9. La question de savoir si les images d'abus d'enfants en ligne constituent une forme de maltraitance limitée à certaines parties du monde où si elles représentent une phase de la progression de la pénétration et de l'utilisation d'Internet reste posée. En d'autres termes, le nombre des images de maltraitance sexuelle impliquant des enfants d'origine asiatique ou africaine augmentera-t-il au fur et à mesure de l'internationalisation de l'accès à Internet ?

Il est difficile d'estimer le nombre de sites Web qui, dans le monde, diffusent des images d'abus d'enfants. En 2010, l'Internet Watch Foundation (IWF) a identifié et mené des actions contre quelque 16 700 cas d'abus sexuels d'enfants sur différentes pages Web du monde entier, contre 10 600 URL de pages Web individuelles ou de sites Web identifiés en 2006<sup>10</sup>. Cette augmentation peut être attribuée à une modification des modèles d'hébergement : au lieu de stocker plusieurs images sur une même page Web, le contenu est publié dans divers emplacements<sup>11</sup>. Plus important encore, le partage des images d'abus d'enfants par des réseaux d'individus aux affinités semblables se multiplie,

grâce à la distribution entre pairs, qui permet de ne pas héberger les images sur des systèmes de stockage détenus par des tiers comme les fournisseurs de services Internet (FSI)<sup>12</sup>.

La manipulation en ligne consiste pour une personne à se lier d'amitié avec un jeune aux fins d'avoir des contacts sexuels en ligne. Une webcam est parfois utilisée, ce qui permet de « partager » cette exploitation au sein de réseaux d'abuseurs sexuels d'enfants. Cette manipulation aboutit parfois à la rencontre physique dans le but d'abuser sexuellement des enfants<sup>13</sup>. Les zones du cyberespace qui permettent aux abuseurs d'abus de manipuler leurs victimes potentielles incluent les forums de discussion interactifs, les sites de réseautage social (SRS) et la messagerie instantanée<sup>14</sup>. Les recherches menées auprès d'abuseurs sur des enfants révèlent que certains d'entre eux ont des listes « d'amis » en ligne pouvant contenir à tout moment jusqu'à 200 noms de jeunes soumis à différents niveaux de manipulation<sup>15</sup>. La manipulation peut prendre quelques minutes, des heures, des jours ou des mois en fonction des objectifs et des besoins de l'adulte maltraitant et des réactions du jeune.

En termes d'âge, les données factuelles rassemblées suggèrent que les enfants qui courent le plus de risques d'être manipulés sont les adolescents et en particulier les adolescentes. À cet âge, les enfants sont souvent des utilisateurs actifs d'Internet qui leur permet de rencontrer des gens et se faire des amis – ce qui fait partie du processus de développement de l'image de soi, y compris de l'identité sociale, sexuelle et émotionnelle.

On ne possède aucune information quant au nombre d'individus (surtout des hommes, d'après les études) qui manipulent les enfants en ligne. Dans de nombreux pays, cette activité ne constitue toujours pas une infraction pénale, ce qui explique pourquoi il n'existe aucune statistique relative à ces comportements. Même dans les pays où la manipulation est pénalisée, il n'existe pas de bases de données coordonnées fournissant des détails sur les délinquants. Ceci constitue une lacune considérable non seulement en matière de connaissances, mais également de protection de l'enfant.

L'abus sexuel d'enfants en ligne et hors ligne suscite de nombreux mythes. Ainsi, on pense souvent que les inconnus représentent la plus grande menace pour les enfants, ce qui s'avère faux en ce qui concerne la création initiale et la distribution d'images d'abus d'enfants. Les responsables directs sont souvent des membres de la famille ou des personnes s'occupant des enfants qui ont un contact physique facile et privé avec ceux-ci<sup>16</sup>. Une autre légende erronée veut que la manipulation soit typiquement le fait d'hommes plutôt âgés, mystificateurs, qui prennent au piège des enfants innocents en utilisant de fausses identités. Il semble

plutôt qu'il s'agisse d'un processus de « séduction » ou de flatterie qui vise à conduire l'enfant à accepter de maintenir une amitié sexuelle en ligne. Même si certains délinquants mentent à propos de leur âge ou de leur genre lorsqu'ils manipulent les enfants, dans la plupart des cas leurs actes relèvent d'un modèle de viol statutaire<sup>17</sup>.

Les données recueillies, découlant pour la plupart d'études menées dans des pays industrialisés, dépeignent la typologie de l'abuseur sexuel sur les enfants en ligne comme étant généralement un homme de type caucasien, économiquement actif, plutôt bien éduqué, dont l'âge varie considérablement et qui peut être lui-même un jeune. Dans de nombreux cas, ceux qui commettent des abus sexuels sur des enfants hors ligne le font également en ligne. Cependant, une proportion importante d'hommes consommateurs d'images d'abus d'enfants en ligne ne semblent pas rechercher le contact sexuel avec les enfants hors ligne<sup>18</sup>. Ce point mérite toutefois d'être analysé avec prudence. Les délinquants ayant accédé à des images d'abus d'enfants en ligne ont montré une certaine forme d'intérêt sexuel pour les enfants et peuvent, par conséquent, présenter un risque physique pour ces derniers. À tout le moins, ils contribuent à soutenir la demande de production d'images d'abus sexuels d'enfants.

Les TIC ont également créé un environnement au sein duquel la pornographie est devenue facilement accessible. L'une des différences clés avec l'ère ayant précédé l'avènement d'Internet est le fait qu'aujourd'hui les jeunes peuvent accéder à de nombreux sites montrant des formes extrêmes de pornographie<sup>19</sup>. Nous ne disposons, à ce jour, que de peu de données factuelles issues de la recherche sur les implications de ce type d'exposition. Les professionnels qui travaillent avec les jeunes se disent de plus en plus inquiets des niveaux apparemment croissants de dépendance vis-à-vis de la pornographie ainsi que des pressions exercées sur les filles afin que celles-ci se conforment à la fois au comportement sexuel et à l'apparence des femmes apparaissant dans les vidéos pornographiques<sup>20</sup>. Les TIC ont également donné lieu à un phénomène d'exposition à une pornographie non sollicitée. L'étendue des troubles que cette exposition suscite chez les enfants semble varier en fonction de l'âge, des normes sociales en vigueur dans leur pays et le degré de contrôle dont ils disposent pour accéder à ces sites<sup>21</sup>.

Les enfants se déclarent très préoccupés par le cyber-harcèlement – également appelé cyber-intimidation ou harcèlement en ligne. Si ce sujet ne semble pas autant inquiéter les adultes que les abus sexuels, on s'y intéresse cependant de plus en plus aujourd'hui<sup>22</sup>. Le harcèlement peut se définir comme tout comportement nuisible ou visant à nuire un enfant, qui se produit à plusieurs reprises et implique un déséquilibre des forces tel qu'il empêche la victime de se défendre ou de mettre fin à ce comportement<sup>23</sup>. Même si le harcèlement est davantage pratiqué hors ligne qu'en ligne, du moins en Europe, Internet

et les téléphones portables offrent aujourd'hui aux enfants et aux jeunes de nouvelles possibilités de harcèlement, plus invasives et anonymes<sup>24</sup>.

Les premiers instigateurs du cyber-harcèlement sont généralement d'autres enfants ou d'autres jeunes. Certaines études suggèrent que les filles sont plus adeptes du harcèlement en ligne que les garçons, mais d'autres études concluent l'inverse<sup>25</sup>. Des études menées au Canada et au Royaume-Uni ont révélé que les enfants risquant d'être intimidés hors ligne (par exemple, les enfants perçus comme « différents », comme ceux appartenant à un groupe ethnique minoritaire, les jeunes lesbiennes, gays, bisexuels ou transgenres, les enfants en surpoids ou encore ceux qui sont atteints de handicaps visibles) courent également un plus grand risque que les autres enfants d'être victimes du harcèlement en ligne<sup>26</sup>. À l'inverse, une étude menée aux États-Unis a montré que ceux qui intimident physiquement les autres à l'école sont également susceptibles d'être eux-mêmes victimes de harcèlement électronique<sup>27</sup>. Si le cyber-harcèlement ne semble pas aujourd'hui être très répandu, il peut exercer un impact significatif sur les enfants et les jeunes en raison de son caractère anonyme, de sa capacité à s'introduire à tout moment du jour ou de la nuit dans des endroits dédiés généralement au délassement et à la vie privée - les maisons et les chambres à coucher - et, de sa tendance à l'expansion, qui se traduit (parfois involontairement) par l'implication et la participation de nombreuses personnes.

### Accès des enfants à Internet

Les données recueillies montrent que la connectivité en ligne des enfants et des jeunes ne cesse de s'accroître. Aujourd'hui, les niveaux d'accès à Internet sont plus élevés dans le monde industrialisé même si les pays à revenu faible et intermédiaire les rattrapent rapidement. Les inégalités sociales affectent l'accès et l'usage d'Internet. Ceux-ci sont plus importants dans les pays prospères en général et parmi les enfants nantis au sein de tous les pays que dans les pays les plus pauvres et parmi les enfants moins privilégiés<sup>28</sup>. Dans la plupart des pays pour lesquels des données sont disponibles, les enfants de moins de 18 ans constituent un pourcentage élevé du nombre total de personnes en ligne<sup>29</sup>. Toutefois, en Europe, le nombre de parents ayant accès à Internet rejoint rapidement le nombre d'enfants qui l'utilisent. En 2008, en moyenne 84 % des parents de cette région avaient déjà utilisé Internet contre 66 % en 200530. Une étude de l'Union européenne (UE) révèle que plus les parents utilisent Internet, plus ils acquièrent des aptitudes complémentaires en la matière et plus ils sont à même de gérer l'utilisation d'Internet par leurs enfants31.

Globalement, la différence de niveau d'utilisation liée au genre n'est pas significative. En revanche, l'âge est un facteur pertinent et l'on constate, en général, une augmentation des niveaux d'accès à Internet

proportionnelle à l'âge des enfants<sup>32</sup>. Toutefois, les plus jeunes sont de plus en plus nombreux à utiliser Internet et l'âge du premier accès à la toile ne cesse de diminuer. Dans l'Union européenne, d'après les informations fournies par les parents, en 2008, 60 % des 6 à 10 ans et 86 % des 15 à 17 ans utilisaient Internet, ce qui représente une augmentation de l'accès par les plus jeunes par rapport aux années précédentes<sup>33</sup>. Dans le monde, le nombre d'enfants qui passent plus de temps en ligne semble s'accroître même si le nombre d'heures d'utilisation varie considérablement. Ainsi, en Europe, les enfants âgés de 9 à 16 ans qui accèdent à Internet passent de une à cinq heures en ligne chaque jour<sup>34</sup>, tandis qu'au Bahreïn, l'accès quotidien s'étend de deux heures et demie à trois heures et demie<sup>35</sup>. En Afrique du Sud, de nombreux utilisateurs d'Internet ne sont en ligne qu'une fois par semaine et pendant moins d'une heure<sup>36</sup>. Au Brésil, 69 % des enfants âgés de 10 à 15 ans accèdent à Internet tous les jours<sup>37</sup>. Toutefois, l'Union internationale des télécommunications (UIT) indique que, en termes de fréquence d'utilisation, le groupe d'âge de 5 à 14 ans est bien moins susceptible d'utiliser Internet au moins une fois par jour (ou presque chaque jour) que la population dans son ensemble ou les jeunes âgés de 15 à 24 ans<sup>38</sup>. Une étude portant sur 9 000 utilisateurs d'Internet adultes et mineurs dans 12 pays dont la Chine, les États-Unis, l'Inde, le Japon et le Royaume-Uni, suggère que les parents sous-estiment le temps que leurs enfants passent en ligne – en moyenne 39 heures par mois, soit deux fois plus que ne le croient les parents. Cette disparité peut s'expliquer par le manque d'engagement, de supervision et de communication des parents avec les enfants. Des exceptions sont à noter au Brésil, en Italie et en Suède, où le temps passé par les enfants sur Internet semble être estimé de manière assez semblable par les enfants et les parents<sup>39</sup>.

Dans les pays industrialisés, la majorité des enfants ont accès à Internet chez eux ou à l'école, alors que dans les pays à revenu plus faible, de nombreux enfants doivent se rendre dans les cybercafés<sup>40</sup>, qui peuvent réunir des utilisateurs adultes et des enfants dans un même espace physique. Au Brésil, par exemple, l'accès à la technologie parmi les enfants âgés de 10 à 15 ans est passé de 53 % à 63 % entre 2008 et 2009. L'accès à partir de cybercafés, tant gratuit que payant, parmi les utilisateurs d'Internet du même groupe d'âge, s'est accru de 33 % en 2006 à 61 % en 2009<sup>41</sup>.

Le paysage de l'utilisation d'Internet se modifie également puisque les téléphones portables deviennent une source d'accès importante. Si, en général, les ordinateurs restent le mode principal d'accès en ligne, le Japon ouvre la voie avec pratiquement 60 % d'enfants qui utilisent désormais leur téléphone pour se rendre sur Internet<sup>42</sup>. Il est probable que l'utilisation par les enfants d'appareils portables permettant l'accès à Internet augmentera progressivement en fonction des conditions socio-économiques des différents pays.

L'explosion mondiale de l'utilisation du téléphone portable est très significative. Les téléphones portables et autres dispositifs mobiles de différents types représentent l'avenir de la connectivité à Internet, en particulier dans les nations à revenu faible et intermédiaire. Il est peu probable que la plupart de ces pays investissent dans l'infrastructure nécessaire pour installer les câbles téléphoniques permettant l'accès à Internet et la connexion de chaque maison. Au contraire, il est vraisemblable qu'ils établiront un réseau WAN (wireless wide area network réseau étendu sans fil) relié ou s'ajoutant aux antennes conventionnelles de téléphonie mobile. L'augmentation de l'utilisation des « smartphones » pour accéder à Internet limitera la capacité des parents à restreindre, surveiller ou contrôler les sites sur lesquels se rendent leurs enfants et représentera un risque potentiel accru pour les enfants et les jeunes. Les téléphones portables sont caractérisés par une immédiateté qui n'existe pas lorsque l'appareil se trouve dans un lieu défini où la surveillance s'exerce plus facilement. Même les téléphones qui ne permettent pas l'accès à Internet fournissent aux jeunes de grandes possibilités de rester en contact ; c'est pourquoi aujourd'hui, dans de nombreux pays industrialisés et à revenu intermédiaire, les jeunes les considèrent comme des outils sociaux indispensables.

Les enfants et les jeunes réalisent un vaste éventail d'activités en ligne - jeux, information, éducation, divertissement et communication. L'UIT rapporte qu'en général, les enfants utilisent plus Internet à des fins éducatives ou ludiques que les autres tranches d'âge tandis que les jeunes et la population en général le font davantage afin de communiquer<sup>43</sup>. Les sites de réseautage social, la messagerie instantanée, les forums de discussion interactifs, les services de microblogage et autres forums permettent aux utilisateurs de mettre en ligne et d'échanger des informations personnelles, des photos et des vidéos, de construire des réseaux d'amis et d'entretenir un haut niveau d'interaction et d'échange d'informations sur tous les aspects de leur vie quotidienne.

Les sites de réseautage social (SRS) sont extrêmement populaires auprès des jeunes qui les considèrent de plus en plus comme faisant partie intégrante de leur vie sociale. Des études menées en Afrique du Sud, en Australie, au Bahreïn, au Brésil, aux États-Unis, au Népal, aux Philippines, ainsi que dans des pays d'Europe sur l'utilisation par les jeunes de ces sites et sur leur comportement en ligne relèvent une utilisation similaire dans la plupart des cas, particulièrement en ce qui concerne l'utilisation des SRS. Ces études révèlent un modèle singulièrement commun d'activités sociales rencontrer des gens, se faire de nouveaux amis et discuter en ligne - ce qui suggère que les facteurs liés au développement de l'enfant et de l'adolescent semblent davantage stimuler la communication en ligne que les facteurs culturels. Aux Etats-Unis, 73 % des adolescents internautes utilisent

aujourd'hui les sites de réseautage social<sup>44</sup>. Dans l'Union européenne, 59 % des enfants de 9 à 16 ans possèdent leur propre profil de réseautage social (ils sont 26 % de 9 à 10 ans et 82 % de 15 à 16 ans)<sup>45</sup>. En Inde, environ 5 % des 37 millions d'utilisateurs de Facebook présumés ont entre 13 et 15 ans et 7 % entre 16 et 17 ans<sup>46</sup>. Au Brésil, Facebook comptait 29 millions d'utilisateurs en octobre 2011 dont 6 % avaient entre 13 et 15 ans et 7 % entre 16 et 17 ans<sup>47</sup>.

# Implications sociales de la fusion des environnements en ligne et hors ligne

Parmi les dimensions-clés de la croissance des activités en ligne, on cite le fait que les enfants et les jeunes participent à un environnement qu'ils contribuent à créer et qui leur fournit un apprentissage, et que les parents dans de nombreuses parties du monde connaissent encore peu ou pas du tout. Un nombre croissant d'enfants créent et explorent aujourd'hui leurs propres réseaux sociaux virtuels. Étant exposés à la publicité en ligne, à des connaissances et des informations, ainsi qu'à des idées politiques, religieuses, culturelles ou sexuelles susceptibles de trancher sérieusement avec celles de leurs parents, leur monde est aujourd'hui considérablement plus complexe. Par conséquent, il faut également craindre que l'extension de l'accès et de l'exposition aux médias électroniques ait des impacts nuisibles, parmi lesquels la diminution potentielle de la capacité des parents de comprendre les expériences vécues par leurs enfants ou de leur offrir une protection et un soutien efficaces<sup>48</sup>. Si le fossé inter-générations lié à l'usage d'Internet commence à se combler dans le monde industrialisé, l'abîme entre les enfants et les parents en matière d'utilisation d'Internet reste profond dans les pays à revenu faible.

Le monde en ligne autorise un mélange complexe d'anonymat individuel, d'autopromotion et de jeux de rôle en fonction des souhaits et désirs de l'utilisateur. Les enfants et les jeunes peuvent définir leurs propres identités en ligne, les modifier et en posséder plusieurs à tout moment. Il en découle une nouvelle dimension de l'interaction sociale, ainsi qu'une nouvelle forme d'espace social, en particulier par le biais des réseaux sociaux qui fournissent de nouvelles possibilités de faire des rencontres et de s'amuser<sup>49</sup>. Si les adultes perçoivent la différence entre les mondes en ligne et hors ligne, chez de nombreux enfants et jeunes qui construisent des réseaux sociaux en se faisant des amis dans ces deux mondes, la distinction est ténue. On peut dire à cet égard que les mondes en ligne et hors ligne ont fusionné.

Les frontières claires utilisées dans le monde physique pour établir une distinction entre les différents aspects ou contextes de la vie n'existent pas ou ne fonctionnent pas nécessairement de la même manière dans le monde en ligne<sup>50</sup>. Les sites de réseautage social utilisent le terme « amis » pour désigner les personnes inclues dans le profil de quelqu'un. D'une part, les limites peuvent sembler d'emblée moins importantes puisque les personnes que l'on rencontre ne sont pas physiquement présentes. Des études menées dans différentes pays du monde suggèrent que les jeunes se sentent souvent plus à l'aise en ligne pour échanger des informations personnelles très personnelles ou s'engager dans des comportements d'ordre sexuel qu'ils ne le seraient hors ligne<sup>51</sup>. D'autre part, les forums en ligne – qu'il s'agisse de forums de discussion interactifs, de blogs, de jeux en ligne ou de sites de réseautage social - démantèlent les frontières traditionnelles de la vie privée. Les enfants participant à des « chats » ou des « discussions » dans l'espace privé de leur propre chambre peuvent s'exposer, volontairement ou involontairement, à un public mondial inconnu, d'où un risque potentiel accru de préjudice. Les informations mises en ligne sont enregistrées et créent un historique de la navigation sur Internet de l'enfant, réduisent le contrôle sur les personnes ayant accès à ses données personnelles et, parfois, le prenne au piège quand il découvre trop tard qu'il ne peut pas retirer ce qu'il a mis en ligne. Les signaux d'alerte qui peuvent permettre de protéger l'enfant dans le monde physique sont pratiquement inexistants en ligne. Le monde physique comprend une série de filtres, comme le langage du corps, le sentiment de défiance éveillé par un « ami » potentiel, ainsi que sa proximité géographique relative. Les nombreux mécanismes développés pour protéger les enfants dans l'environnement hors ligne n'existent pas encore dans le monde en ligne.

# Comprendre le risque, la vulnérabilité et le préjudice

Il existe des différences majeures entre le risque et le préjudice dont les responsables politiques et les parents doivent prendre conscience. Certains types d'activités peuvent impliquer des risques ne débouchant pas nécessairement sur un préjudice portant atteinte aux enfants et aux jeunes. La natation, la pratique de la bicyclette ou la participation à un site de réseautage social peuvent être positifs mais font également courir des risques et, dans certaines circonstances, peuvent exposer l'enfant à un préjudice. Plus spécifiquement, en ce qui concerne Internet, il n'est pas facile de tracer une frontière claire entre les activités apportant des bienfaits et celles entraînant des risques<sup>52</sup>.

Souvent, les adultes sont inquiets des risques que font courir les informations et les images publiées en ligne. C'est la raison pour laquelle la majorité des recherches partent du principe que mettre des informations en ligne constitue, en soi, un comportement à risque. En effet, les jeunes partagent des informations que les adultes

peuvent estimer gênantes. De nombreuses données factuelles émanant de l'ensemble du globe révèlent que de nombreux jeunes, en particulier ceux âgés de 12 à 16 ans, mettent en ligne des informations extrêmement personnelles. Au Brésil, par exemple, des études ont montré que 46 % des enfants et des adolescents considèrent qu'il est normal de publier régulièrement des photos personnelles sur Internet, tandis qu'une étude menée au Bahreïn indique que les enfants placent généralement des informations personnelles en ligne sans avoir aucune notion du concept de respect de la vie privée<sup>53</sup>. En outre, un nombre important d'adolescents téléchargent des représentations visuelles à tonalité sexuelle les mettant en scène<sup>54</sup>. Parfois, ils agissent en réponse à une manipulation qui les encourage à placer ce type d'images en ligne et qui peut être suivie de chantage ou de menaces d'exposition afin de forcer ces adolescents à télécharger un nombre toujours croissant d'images explicites. Dans d'autres cas, le placement initial n'est pas sollicité et peut encourager et attirer des prédateurs potentiellement malfaisants.

Parmi les autres comportements courants chez les adolescents, citons le « sexting » (partage d'images ou de textes à connotation sexuelle par téléphone portable)<sup>55</sup>. Ces images et textes sont souvent partagés avec des partenaires avec qui une relation est maintenue ou avec des partenaires potentiels mais il arrive qu'un public nettement plus large finisse par y accéder<sup>56</sup>. Il est peu probable que les jeunes adolescents évaluent correctement toutes les implications de ces comportements et les risques potentiels qu'ils présentent.

Toutefois, la mise en ligne d'informations fait l'objet d'un vaste débat. On peut faire valoir que publier des informations personnelles en ligne est devenu un comportement considéré comme normal<sup>57</sup>. En effet, la page d'un jeune qui ne comporterait pas d'informations personnelles serait considérée par ses pairs comme sans charme et sans intérêt. Ces derniers auraient même tendance à prendre cet enfant pour quelqu'un d'un peu bizarre ou en retrait. Mettre des informations en ligne fait partie de leur mosaïque culturelle ; cette activité est monnaie courante et la majorité des jeunes ne semble pas en souffrir<sup>58</sup>. Une recherche menée aux États-Unis, a ainsi révélé qu'en général, il n'existe que peu de preuves suggérant que le placement en ligne quotidien d'informations personnelles, y compris d'images, entraîne une victimisation personnelle des enfants. C'est l'interaction et l'engagement en ligne dans différents types de comportements à risque, plutôt que le partage d'informations, qui créent l'environnement propice à l'apparition des abus sexuels et de la manipulation<sup>59</sup>. Il est irréaliste de tenter de modifier des comportements normatifs et, en outre, les données recueillies suggèrent qu'il n'est probablement ni utile ni nécessaire de le faire.

Les données factuelles disponibles sont insuffisantes pour fournir une réponse sans aucune ambiguïté à la question de savoir si les risques associés aux activités en ligne sont les mêmes ou ont des implications semblables pour les enfants dans différentes régions du monde. Par exemple, dans de nombreux pays africains et asiatiques, le niveau de pauvreté et la faiblesse des structures de l'État sont tels que la protection sociale et juridique des enfants n'est pas assurée et qu'ils sont susceptibles de contribuer à accroître leur vulnérabilité<sup>60</sup>. Les observations sur les autres caractéristiques particulières susceptibles de rendre les enfants vulnérables à l'abus et à l'exploitation sexuels en ligne sont contradictoires. Des recherches menées en Afrique du Sud et aux États-Unis suggèrent que l'enfant ayant une faible estime de soi, dépressif, ayant subi des revers, victime d'abus hors ligne ou de persécution coure un risque réel d'être manipulé en ligne<sup>61</sup>. Les conclusions d'études menées au Royaume-Uni ne rapportent, quant à elles, aucun modèle évident de vulnérabilité spécifique dans le monde hors ligne<sup>62</sup>. Une étude brésilienne a découvert un lien important entre les acteurs sociaux et la situation économique. Les filles habitant les favelas (bidonvilles) sont exposées à la sexualisation précoce et plus susceptibles de se socialiser avec des groupes plus âgés qu'elles considèrent comme des vecteurs d'élévation de leur statut social. Elles ont indiqué que, pour elles, Internet est un instrument qui leur permet de consulter des sites à orientation sexuelle et de rencontrer des garçons. Les jeunes Brésiliennes de classe moyenne, par contre, qui semblent bénéficier d'une meilleure surveillance et supervision de la part des adultes que les filles des favelas, ont déclaré utiliser Internet principalement à des fins éducatives<sup>63</sup>.

De plus, dans les pays à revenu faible, les enfants sont moins susceptibles d'utiliser Internet à domicile et, s'ils le font, leurs parents sont probablement bien moins avertis de la nature et des risques liés à l'environnement en ligne, ce qui réduit les possibilités de protection et de soutien parental. Les enfants qui accèdent à Internet dans les cybercafés au Brésil, en Inde, au Népal et aux Philippines qualifient ces endroits de particulièrement dangereux, les exposant potentiellement à des adultes adeptes de la pornographie, à du matériel pornographique, à des sollicitations ou aux drogues. En corollaire, dans les pays où les enfants accèdent à Internet essentiellement dans les cybercafés, il y a généralement moins de réglementation, moins de possibilités de porter plainte et, dans de nombreux cas, un investissement global extrêmement limité dans la construction d'un environnement protecteur<sup>64</sup>. Néanmoins, il est évident que même si utiliser Internet chez soi peut sembler moins dangereux, il serait plus exact de dire que si certains dangers sont réduits ou écartés à domicile, d'autres dépendent du type d'activités en ligne que pratiquent les enfants.

Certaines des études disponibles ventilent les données en fonction du genre, fournissant ainsi de précieuses informations sur les différences et les similarités en matière de risques, de vulnérabilité et de préjudices subis par les garçons et les filles. Toutefois, il n'existe aucune donnée empirique concernant un grand nombre de groupes. Par exemple, les TIC peuvent présenter de nombreux bénéfices potentiels pour bien des enfants souffrant d'un handicap, comme la communication pour ceux qui sont incapables de se déplacer librement dans le monde physique, un meilleur accès aux textes écrits pour les enfants ayant un handicap visuel et une capacité de communiquer aisément pour les enfants malentendants. Pourtant, on ne sait pas si les enfants handicapés courent un plus grand risque d'être dépendants des relations en ligne et s'ils sont par conséquent plus vulnérables, et s'ils ressentent un désir plus grand de construire des identités alternatives que les autres enfants ou s'ils sont plus susceptibles d'être visés par la manipulation. Pareillement, les jeunes lesbiennes, gays, bisexuels et transgenres (LGBT), en particulier s'ils vivent dans des environnements qui ne leur permettent pas d'exprimer ouvertement leur sexualité, ont beaucoup à gagner à se servir d'Internet pour se lier d'amitié avec des personnes partageant leur orientation sexuelle. À l'inverse, une forte dépendance à Internet pourrait les exposer aux risques d'abus. Un certain nombre de données montre que les jeunes LGBT sont particulièrement vulnérables au cyber-harcèlement<sup>65</sup>. Vu l'importance que revêtent les relations parentales pour soutenir et protéger les enfants, il serait également d'un grand intérêt de mener des études pour mieux comprendre les risques auxquels les enfants immigrés ou séparés de leurs familles sont exposés dans l'environnement en ligne.

Quant à savoir si les jeunes sont conscients des risques qu'ils courent en ligne, des études menées au Brésil et dans certains pays d'Europe suggèrent que de nombreux enfants connaissent les dangers de base mais que la plupart d'entre eux ne se perçoivent pas comme vulnérables. Les enfants pensent que « les autres » (par exemple, les enfants plus jeunes ou non-expérimentés) sont exposés à des risques, mais pas eux-mêmes<sup>66</sup>. Bien des enfants et des jeunes qui se rendent sur les sites de réseautage social sont conscients des défis relatifs à la sécurité de l'information, se sont sentis contraints de publier des informations personnelles alors qu'ils n'avaient pas envie de le faire et ressentent une certaine crainte à l'idée d'être visibles par tant de personnes qu'ils ne connaissent pas. Pourtant, une enquête menée à l'échelle du Royaume-Uni indique que ceci n'a que peu d'impact sur leur comportement à moins qu'un problème ne les ait touchés personnellement ou se soit révélé grave<sup>67</sup>.

Globalement, les dangers liés à Internet sont perçus de manières extrêmement différentes par les enfants et les jeunes. Même si l'on ne dispose que de très peu de recherches comparatives capables de montrer la manière dont naissent ces différentes perceptions, elles semblent associées à la disponibilité de l'information, au lieu d'utilisation

et à la prise de conscience de mécanismes d'information sûrs.

### Parents ou pairs : à qui les enfants demandent-ils de l'aide ?

La recherche menée dans le monde entier indique que les enfants et les jeunes ont bien plus confiance dans leurs propres capacités à garantir leur sécurité en ligne que dans celles de leurs parents<sup>68</sup>. Globalement, cependant, les enfants ne font pas preuve de la même confiance dans les pays où les informations relatives à la sécurité sur Internet ne sont pas largement disponibles. Une recherche européenne de 2009 est arrivée à la conclusion que les parents ont moins tendance à s'inquiéter de la sécurité en ligne de leurs enfants s'ils utilisent euxmêmes Internet. Une fois qu'ils comprennent mieux l'environnement en ligne, les parents ont une vision éclairée des risques encourus<sup>69</sup>.

Quant à la protection contre les préjudices, les données recueillies indiquent généralement que, souvent, les enfants victimes d'abus ne se tournent pas automatiquement vers leurs parents en premier lieu. Le niveau d'implication des parents varie, cependant, en fonction de différents facteurs y compris le pays, l'âge et leur propre niveau d'utilisation d'Internet<sup>70</sup>. Les raisons pour lesquelles les enfants ne s'adressent pas à leurs parents pour se protéger des préjudices en ligne sont de plusieurs ordres : ils pensent que leurs parents ne comprennent pas le monde dans lequel l'abus s'est produit, craignent de se voir confisquer leur téléphone portable ou restreindre leur accès à Internet, sont confrontés à des menaces proférées par l'abuseur ou redoutent la honte et l'humiliation<sup>71</sup>. Quel que soit le souhait des parents, certains adolescents ne veulent pas que les adultes interviennent. L'adolescence est souvent un stade de développement où le jeune adopte un comportement d'exploration et de distanciation, jusqu'à un certain degré, avec ses parents. Par conséquent, les adolescents perçoivent la présence des parents et leur implication dans leur espace social et leurs interactions en ligne comme autant d'interférences.

Néanmoins, un nombre croissant de données factuelles émanant du monde industrialisé révèle que le facteur le plus à même de protéger les enfants est la présence de parents activement engagés qui partagent des expériences sur Internet avec leurs enfants et sont disposés à parler avec eux des risques qu'il implique<sup>72</sup>. Le respect et l'intérêt portés à la participation des enfants à l'environnement en ligne sont apparemment plus efficaces que les contrôles restrictifs ou punitifs. De plus, des éléments de recherche suggèrent que de nombreux enfants et jeunes aimeraient que leurs parents s'impliquent davantage. Pour de nombreux enfants, l'exclusion des parents ne semble pas dériver inévitablement de leur réticence à demander de l'aide, mais plutôt de la perception qu'ils ont

de la capacité limitée des parents de fournir une aide efficace<sup>73</sup>.

La capacité des parents à protéger les enfants est également de plus en plus limitée par le fait que de nombreuses activités exercées précédemment sur des ordinateurs basés à un endroit déterminé sont aujourd'hui pratiquées sur des téléphones portables dotés d'une connexion à Internet. Si les enfants ont accès à ce type de téléphone – ce qui est de plus en plus le cas – les parents sont moins en mesure de surveiller les activités des enfants, d'introduire des filtres, de bloquer des mécanismes ou de contrôler le degré d'accès à Internet. Ce nouveau modèle d'utilisation lance des défis fondamentalement différents qui doivent être pris en compte dans la mise en place de stratégies de protection ou de prévention.

Le message clair qui se dégage des recherches indique que les enfants et les jeunes se considèrent comme les « protecteurs » des autres enfants. Les enfants ont tendance, dans un premier temps, à se tourner les uns vers les autres lorsqu'ils ont besoin d'aide. Les jeunes font très attention et sont sensibilisés aux risques que courent leurs jeunes frères et sœurs, leurs amis et les autres enfants qu'ils perçoivent comme plus vulnérables qu'euxmêmes<sup>74</sup>. On peut en déduire que les enfants jouent le rôle potentiel de pairs éducateurs, de mentors et de conseillers. Dans le contexte sociologique de l'utilisation actuelle d'Internet, être à l'écoute des enfants et les soutenir dans leur volonté d'être les premiers à prendre soin d'eux-mêmes et des autres constituent probablement l'une des clés pour réduire tant le risque que le préjudice.

L'usage que font les enfants d'Internet, le comportement qu'ils y adoptent et les vulnérabilités qu'ils subissent dans l'environnement en ligne diffèrent en fonction de leur âge. Il est essentiel de reconnaître l'évolution des capacités des enfants en adoptant des stratégies de protection appropriées à leur âge et à leur niveau de compréhension. Jusqu'ici, on ne sait que peu de choses sur l'expérience en ligne des plus jeunes enfants même si un corpus croissant de données montre que, dans les pays industrialisés, de nombreux enfants de moins de huit ans ont aujourd'hui accès à Internet par le biais d'ordinateurs ou de téléphones portables. De nouvelles études doivent se pencher sur cette utilisation par les plus jeunes et sur les mesures à adopter pour protéger les enfants d'âges et de capacités différentes.

Le défi à relever par les partisans de la protection exercée par les adultes consiste à démontrer que ce modèle peut être efficace dans le contexte d'un monde en ligne en rapide évolution, en particulier dans les cas où les parents n'ont qu'une connaissance lacunaire d'Internet, ainsi que du rôle qu'il joue dans la vie de leurs enfants. À l'inverse, le défi pour ceux qui préfèrent faire confiance aux enfants consistera à démontrer que cette confiance est bien placée et que les enfants sont socialement et techniquement en mesure de veiller sur eux-mêmes et sur les

autres. En réalité, ces deux approches doivent se renforcer mutuellement.

Les programmes destinés à aider les enfants et les jeunes à faire des choix éclairés sur la base d'une prise de conscience réelle de la nature des risques qu'ils courent doit s'accommoder de la compréhension de la sexualité des adolescents, du rôle des groupes de pairs, des attentes culturelles des adolescents et de l'estimation des risques du point de vue des enfants et des jeunes. Les messages de mise en garde doivent, par exemple, mettre l'accent sur les problèmes pouvant découler de l'interaction avec des personnes rencontrées en ligne au lieu de formuler des messages de prévention que comprennent les adultes mais qui ne correspondent pas à l'utilisation normative ou à la nature du risque tel que le perçoivent les jeunes<sup>75</sup>. Par exemple, un de ces messages pourrait dire: « ne publiez pas d'informations

personnelles ». Les risques en ligne peuvent être réduits pour autant que des mécanismes externes soient mis en place pour réglementer l'environnement, que des relations de confiance et de soutien s'établissent avec les parents et que celles-ci s'accompagnent des connaissances, des compétences et de la prise de conscience nécessaires pour permettre à l'enfant ou au jeune de naviguer efficacement dans l'environnement en ligne.

La responsabilité de protéger les enfants dans l'environnement en ligne n'incombe pas seulement aux parents et aux enfants. Les responsables politiques, les professionnels, comme les enseignants et les assistants sociaux, les services chargés de l'application des lois et le secteur privé ont tous un rôle à jouer dans la création d'un environnement extérieur sûr permettant aux enfants et aux jeunes de bénéficier de l'utilisation des technologies modernes sans subir de préjudice.

# **DEUXIÈME PARTIE**

# CONSTRUIRE UN ENVIRONNEMENT PROTECTEUR



Il reste beaucoup à faire dans toutes les régions du monde industrialisé de même que dans les pays à revenu faible et intermédiaire. Pour donner une réponse globale au problème de la protection, il faut mettre en œuvre des actions impliquant une diversité d'acteurs gouvernementaux et non gouvernementaux dans un éventail de domaines. Ceci comprend la mise en place d'une « architecture » – un cadre législatif définissant les activités criminelles, la capacité de dissuader les abuseurs potentiels et de poursuivre les délinquants, ainsi que des mesures proactives pour restreindre et proscrire l'accès à des images abusives d'enfants par les délinquants réels et potentiels. Ces actions incluent également le renforcement du travail conjoint et de la collaboration intersectorielle entre la protection sociale et la justice. Il est important d'améliorer la sensibilisation des services de protection des enfants, d'informer les autres professionnels qui travaillent avec les enfants, comme les enseignants, sur la nature des risques et des délits que présentent les mondes en ligne et hors ligne fusionnés et d'instaurer des mesures de soutien pour garder les enfants en sécurité. Il est essentiel de promouvoir des stratégies permettant aux enfants de se prémunir contre les préjudices. L'investissement dans des mesures de protection sociale est requis pour répondre aux besoins des enfants ayant subi des préjudices dus à l'exploitation sexuelle et des abus commis sur Internet et pour renforcer les compétences des professionnels qui travaillent avec eux.

Compte tenu de son rôle central dans la conception et le développement d'Internet, le secteur privé ne peut qu'admettre que sa contribution au vaste objectif social que constitue le fait de rendre Internet plus sûr pour les enfants et les jeunes est intrinsèque à l'élargissement de l'accès et à l'innovation des contenus. Comme Sonia Livingstone et Leslie Haddon l'ont souligné, plus l'utilisation d'Internet se personnalise, plus le rôle des parents ou des enseignants se complique, ce qui accroît la responsabilité de l'industrie dans la gestion des risques que peuvent rencontrer les enfants<sup>76</sup>. À défaut de l'assumer, l'industrie s'expose à une réglementation gouvernementale ou régionale qui exercera un impact négatif sur les

libertés symbolisées par Internet tel que nous le connaissons aujourd'hui.

Une vaste réponse nécessite de travailler directement avec les jeunes dans la conception et la mise en œuvre de stratégies d'information et de protection. Les enfants et les jeunes doivent être informés des risques et de la manière de les éviter, ainsi que des mécanismes et voies à suivre s'ils se trouvent dans des situations qu'ils jugent douteuses. Ils ont besoin de compétences pour opérer des choix éclairés concernant leurs activités dans le cyberespace et pour se fournir mutuellement de l'aide. Cette démarche gagne en importance au fur et à mesure que l'usage d'Internet devient plus privé (c.-à-d. qu'il se produit dans les espaces privés des enfants, tels que les chambres à coucher, comme c'est le cas dans une grande partie du monde industrialisé) et plus mobile. Les mécanismes de protection des enfants doivent être transparents, accessibles et adéquats. S'ils sont censés les utiliser, les enfants doivent se sentir en sécurité et les percevoir comme efficaces. La participation active des enfants aux stratégies de protection en ligne fournit une source essentielle d'expérience et d'expertise.

Renforcer la capacité des parents à soutenir leurs enfants constitue également une composante vitale de la sécurité en ligne. S'il ne faut pas imputer l'entière responsabilité de la protection aux enfants et aux parents, force est de reconnaître l'évidence. La nature de l'espace social fourni par Internet et le fait que les jeunes sont les pionniers de son exploration et de son utilisation impliquent de les mettre à l'avant-plan des solutions visant à réduire les risques ; quant aux parents, ils occupent incontestablement une position de choix pour les soutenir. Les parents doivent être conscients de la nature des risques et être encouragés à améliorer leur compréhension des activités en ligne des jeunes.

Dans le monde industrialisé – à un degré plus ou moins important selon les pays – certains de ces éléments sont réunis. Cependant, il est nécessaire de mieux coordonner les actions entre elles. Dans de nombreux pays à revenu faible et intermédiaire, la prise de conscience de la nature du risque et

des capacités à le réduire ou à y répondre n'en est au mieux qu'à ses premiers balbutiements. Par sa nature même, l'abus sur Internet n'a pas de frontières; une action internationale coordonnée par les secteurs de la justice et du bien-être social s'impose par conséquent.

# Instruments et engagements internationaux

À l'instar d'un certain nombre d'autres questions de protection des enfants, les abus et l'exploitation des enfants en ligne se situent à l'intersection de deux ensembles de normes internationales. Globalement, ils fournissent un cadre pour répondre au phénomène et documenter la création d'un environnement protecteur pour les enfants. D'une part, certains instruments internationaux se concentrent sur les abus et l'exploitation qu'ils considèrent comme une violation des droits de l'enfant, tout en l'inscrivant dans le contexte plus large de la promotion et la protection des droits de l'enfant, interdépendants et indivisibles. D'autre part, plusieurs instruments internationaux visent à répondre à diverses formes de criminalité transnationale et ciblent davantage la riposte et la poursuite tout en tenant compte des droits fondamentaux des personnes lésées.

Dans ce contexte, les cinq principaux instruments internationaux sont :

- La Convention relative aux droits de l'enfant (1989).
- Le Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants (OP-CRC-SC, 2000).
- Le Protocole visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée (« Protocole de Palerme », 2000).
- La Convention du Conseil de l'Europe sur la cybercriminalité (2001).
- La Convention du Conseil de l'Europe sur la Protection des enfants contre l'exploitation et les abus sexuels (2007).

Non seulement ces instruments suggèrent des manières d'aborder et de réagir à l'exploitation et aux abus sexuels d'enfants dans l'environnement en ligne, mais en outre, ils instaurent un ensemble d'obligations juridiquement contraignantes pour que les États parties prennent des mesures précises à cet égard. Ensemble, ils élaborent un cadre complet des droits de l'enfant, définissent les infractions, mettent en place des dispositions qui exigent la sanction des comportements pénalisés et permettent la poursuite

plus efficace des auteurs. La Convention relative aux droits de l'enfant revêt une importance particulière puisqu'elle met sur le même plan la protection des enfants et d'autres droits particulièrement pertinents liés aux avantages apportés par Internet – la liberté d'expression, la liberté de rechercher des informations et la liberté d'association. L'OP-CRC-SC et la Convention du Conseil de l'Europe sur la Protection des enfants contre l'exploitation et les abus sexuels proposent des exemples complets de mécanismes juridiques invitant les gouvernements à mettre en œuvre et à assurer une offre de services pour aider les enfants victimes et leurs familles.

Même si les instruments régionaux s'appliquent spécifiquement au sein de la région dans laquelle ils sont développés, ils établissent des normes ou des points de repère susceptibles d'être adoptés par d'autres pays qui peuvent choisir de s'y conformer, voire, dans certains cas, d'être ratifiés par des États extérieurs à la région. Si le droit international impose aux États la responsabilité première d'assurer le respect, la promotion et la protection des droits de l'enfant, la Convention relative aux droits de l'enfant et les instruments supplémentaires reconnaissent à d'autres acteurs – tels que les parents, la société civile, les fournisseurs d'accès et les entreprises du secteur privé – une responsabilité capitale à cet égard.

Depuis les années 1990, l'Organisation des Nations Unies et les organismes qui lui sont associés, de même que diverses organisations régionales, ont pris des engagements supplémentaires et ont adopté des lignes directrices et des codes de conduite visant à renforcer les mécanismes de protection de l'enfant. Le progrès s'est accéléré avec la nomination, en 1990, par la Commission des droits de l'homme, du Rapporteur spécial sur la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants et l'adoption par la Commission en 1992 d'un Programme d'Action, puis par l'organisation de trois Congrès mondiaux sur l'Exploitation sexuelle des enfants (Stockholm, 1996; Yokohama, 2001; Rio de Janeiro, 2008), qui ont réaffirmé l'objectif, axé sur les droits de l'homme, de protection universelle des enfants contre toutes formes d'exploitation sexuelle<sup>77</sup>.

À cet égard, en 2008, le troisième Congrès mondial a débouché sur la déclaration de Rio qui appelle les États à entreprendre des actions spécifiques et ciblées pour prévenir et éradiquer les images abusives d'enfants, ainsi que l'utilisation d'Internet et des nouvelles technologies aux fins de manipulation des enfants dans le but d'en abuser en ligne et hors ligne, de produire et de diffuser des images abusives d'enfants et d'autres matériaux<sup>78</sup>. L'étude précédente de l'ONU sur la violence contre les enfants, dont le rapport a été présenté à l'Assemblée générale des Nations Unies en 2006, a également reconnu la nécessité « pour les gouvernements de renforcer les mesures visant à lutter contre l'utilisation des technologies de

l'information... dans l'exploitation sexuelle des enfants et d'autres formes de violence »<sup>79</sup>.

Cependant, en dépit de l'accent mis au niveau international sur l'exploitation sexuelle et les abus d'enfants et du développement de ces nouveaux instruments mondiaux et régionaux des droits de l'homme, le défaut de mise en œuvre systématique au niveau national de la législation indispensable et des actions qui devraient en découler reste flagrant. Par exemple, dans son examen toujours en cours des lois liées à la « pornographie mettant en scène des enfants », l'International Centre for Missing & Exploited Children a indiqué qu'en 2010, seuls 45 pays sur les 196 étudiés possédaient une législation suffisante pour lutter contre les délits liés aux images abusives d'enfants, tandis que 89 d'entre eux n'avaient mis en place aucune législation visant spécifiquement la pédopornographie. Parmi les pays qui possèdent une législation de ce type, 52 ne définissent pas la pédopornographie (ou pornographie mettant en scène des enfants) dans leur législation nationale, 18 ne s'occupent pas des infractions liées à l'ordinateur et 33 ne pénalisent pas la possession de matériel pédopornographique, qu'il y ait ou non intention de diffuser celui-ci<sup>80</sup>.

Au niveau régional, l'Union européenne a reconnu la nécessité d'une action collective dans la lutte contre les abus et l'exploitation sexuels des enfants, arguant que même si la législation nationale couvre certaines de ces questions, elle ne traite pas des abus et de l'exploitation sexuels des enfants par le biais des TIC et n'est ni assez sévère ni assez cohérente pour fournir une réponse et une protection efficaces aux enfants qui en sont victimes<sup>81</sup>.

En conséquence, en novembre 2011, l'UE a adopté la Directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, qui remplace la décision-cadre 2004/68/JAI. Parmi d'autres actions, la Directive pénalise les formes d'abus et d'exploitation sexuels des enfants actuellement non couvertes par la législation européenne, telles que la manipulation, les représentations pornographiques en ligne et la visualisation de pédopornographie sans téléchargement de fichiers ; elle abaisse les seuils pour l'application de peines maximales ; elle veille à ce que les délinquants ressortissants de l'UE soient passibles de poursuites pour les crimes commis à l'extérieur de l'UE ; elle fournit aux enfants victimes de ces délits une aide, un soutien et une protection, y compris pour réclamer des indemnités ; elle partage les données relatives aux condamnations criminelles des délinquants sexuels entre les autorités compétentes des États membres ; enfin, elle introduit le retrait obligatoire ou le blocage éventuel de l'accès aux sites Web contenant du matériel à caractère pédopornographique82.

L'UE a toujours été favorable à l'autoréglementation comme moyen d'assurer la sécurité en ligne des jeunes. En février 2007, les principaux opérateurs mobiles et fournisseurs d'accès de l'UE ont adopté un cadre européen pour une utilisation plus sûre des téléphones portables par les adolescents et les enfants. En juin 2010, 25 États membres de l'UE disposaient de codes de conduite tandis que les deux autres les mettaient au point. Le cadre soumet ses signataires à des principes et des mesures, parmi lesquels citons le contrôle d'accès des contenus pour adultes, les campagnes de sensibilisation visant les parents et les enfants, ainsi que la classification des contenus commerciaux conformément aux normes nationales de décence et d'à propos. Un rapport de mise en œuvre paru en juin 2010 conclut à l'efficacité du cadre et constate que 83 opérateurs de téléphonie mobile, desservant 96 pour cent des clients européens de mobilophonie, mettent le cadre en place par le biais des codes de conduite83.

En février 2009, soit deux ans après l'adoption du code pour une utilisation plus sûre des téléphones mobiles, la Commission européenne a collaboré à la réalisation d'un document intitulé *Principes* de l'UE pour des réseaux sociaux plus sûrs avec 21 signataires de tous ou des plus grands SRS opérationnels dans les 27 États membres. Les principaux objectifs de ces principes concernent les paramètres de confidentialité, mais également des dispositions importantes liées à des activités éducatives et de sensibilisation ainsi qu'au signalement des abus. Une deuxième évaluation des principes de réseautage social a été publiée en mai 2011. Les conclusions de ce dernier rapport sont plus mitigées : sur les 14 SRS qui ont répondu au sondage, 3 seulement ont reçu de bonnes notes dans des matières comme la formulation explicite des caractéristiques (p. ex., catégorie d'âge visée, disponibilité, convivialité, etc.) ou les paramètres de confidentialité<sup>84</sup>.

En juin 2011, la Commission européenne a tenu sa première Digital Agenda Assembly (Assemblée de la Stratégie numérique). Cette rencontre proposait un atelier spécifique intitulé « Every European Child Safe Online » au cours duquel Digital Europe, association commerciale regroupant un large éventail d'entreprises de haute technologie, a présenté une proposition de projet afin de développer un nouveau cadre de haut niveau portant sur les droits et les responsabilités.

S'il n'existe aujourd'hui aucun protocole interaméricain ni instrument spécifique à la protection des enfants dans les environnements en ligne et hors ligne, à l'échelle régionale, en revanche, on dispose de ressources régionales pertinentes. La « Déclaration de Montevideo », formulée en juillet 2009 par un groupe d'experts régionaux, fournit un cadre pour la protection des renseignements personnels des enfants dans le cyberespace<sup>85</sup>. Conçu pour guider les législateurs, les juges, les décideurs et les services chargés de l'application des lois en matière de protection des données personnelles des enfants en ligne,

la Déclaration énumère des recommandations sur la prévention et l'éducation, les cadres juridiques, l'application de la loi et les politiques publiques <sup>86</sup>. Même si la Déclaration n'a pas force obligatoire dans aucun État d'Amérique latine, elle constitue un cadre essentiel pour les États qui cherchent à protéger les renseignements personnels des enfants en ligne. En Afrique, en Asie et au Moyen-Orient, une coordination régionale a été mise en place, mais elle est généralement adaptée aux besoins du moment.

# Défis en matière d'application des lois et de protection des enfants

S'ils revêtent une importance fondamentale, la législation et les engagements politiques ne suffisent pas à apporter le changement s'ils ne s'accompagnent pas de mécanismes qui en assurent la mise en œuvre et l'application, ainsi que de services destinés à fournir aux victimes le soutien nécessaire. Les services chargés de l'application des lois, quant à eux, assument la responsabilité de veiller à ce que les lois soient appliquées avec cohérence et efficacité et à ce que les délinquants soient poursuivis et rendent des comptes. Ils jouent donc un rôle capital en s'attaquant à l'exploitation et aux abus sexuels d'enfants dans les environnements en ligne/hors ligne fusionnés. Aux organismes de protection sociale, il incombe de promouvoir et de protéger l'intérêt supérieur des enfants victimes d'abus. Cependant, ces deux finalités peuvent parfois entrer en conflit. L'enjeu consiste à explorer des approches à la fois efficaces pour mettre en œuvre les poursuites tout en assurant que les intérêts individuels des enfants concernés restent la priorité absolue.

L'environnement en ligne du XXIe siècle a transformé la criminalité de plusieurs manières : en tant que mode de communication révolutionnaire, il a créé un espace transnational offrant de nouvelles possibilités d'activités répréhensibles. De plus, la nature virtuelle de l'environnement en ligne permet parfois à l'activité criminelle d'échapper à la compétence du système de justice pénale<sup>87</sup>. La prévention du crime ne peut plus se contenter d'opérer une surveillance et de mener l'enquête au sein de la collectivité proche : elle doit traverser les frontières locales, nationales et internationales. Il peut s'avérer difficile de désigner les tribunaux compétents pour juger d'un crime commis dans l'environnement virtuel. Ajoutons que certains crimes portent parfois préjudice à plusieurs victimes se trouvant dans différents pays, ce qui complique singulièrement les procédures de protection des enfants. Les crimes liés aux abus et à l'exploitation sexuels commis en ligne peuvent être le fait de délinquants qui agissent à des milliers de kilomètres de leurs jeunes victimes. Tout cela représente d'importants défis et exige une plus grande collaboration entre les forces de l'ordre des

différents pays ayant des protocoles de compétence, des milieux sociaux et culturels, des attentes politiques et des niveaux d'aptitudes, d'expertise technique et de ressources variés<sup>88</sup>.

Établir qu'un crime relevant de l'exploitation ou de l'abus sexuel en ligne des enfants a été commis est souvent complexe. L'une des caractéristiques uniques de l'environnement en ligne est le fait qu'il n'est pas nécessaire qu'un contact physique se produise entre l'enfant et le délinquant pour qu'un délit soit commis. Les défis auxquels sont confrontés les services chargés de l'application des lois sont particulièrement délicats lorsque la législation ne fournit pas de définition précise de l'activité criminelle. Par exemple, pour affirmer qu'un délit a été commis est-il suffisant de montrer « l'intention » de leurrer l'enfant même si aucun contact physique réel n'a été établi ; quelle preuve de « l'intention » est nécessaire ; en quoi consiste une image pédopornographique? Certains États, comme le Royaume-Uni et le Canada, criminalisent les images simulées ou réelles montrant des enfants participant à une activité sexuelle.

Les enfants apparaissant sur des images abusives ou manipulés en vue d'être exploités sexuellement peuvent éprouver des sentiments de honte et de complicité. Par conséquent, beaucoup de victimes de délits commis sur Internet ne révèlent pas leurs expériences jusqu'à ce que les images ou les vidéos soient découvertes, le plus souvent par les services chargés de l'application des lois, dans le cadre d'une enquête. Et même dans ce cas, la situation reste complexe. Il arrive que l'enfant victime des abus continue à nier et refuse de reconnaître qu'il a été filmé même si les services chargés de l'application des lois sont en possession d'images de maltraitance le mettant en scène<sup>89</sup>.

La plupart des abus sexuels commis sur des enfants ne sont jamais dévoilés. Si l'abus a lieu en ligne, le secret est d'autant mieux gardé 90. Certains enfants maltraités perçoivent les personnes avec lesquelles ils ont eu une relation en ligne comme leur petit-ami ou petite-amie et en deviennent émotionnellement dépendants. D'autres enfants soumis à la manipulation, se sentant isolés et démunis de soutien social, sont peu enclins à rapporter les faits aux services chargés de l'application des lois ou autres. Ajoutons à cela que bien des enfants ne se rendent pas compte qu'ils ont été les victimes d'un délit parce que des images innocentes d'enfants peuvent être transformées numériquement en matériel pornographique et être distribuées sur Internet à l'insu de la victime<sup>91</sup>.

La divulgation des abus achoppe sur plusieurs défis souvent sous-estimés et mal compris. Les enfants ont besoin que leurs sentiments et craintes soient reconnus pour faire face à cette expérience. Il n'est pas inhabituel que les enfants reviennent sur leurs déclarations de peur des répercussions qu'elles pourraient avoir sur eux-mêmes, leur famille ou d'autres personnes importantes dans leurs vies et sur l'auteur de l'abus. Les enfants sont non seulement affectés par l'abus lui-même, mais peuvent également être traumatisés par sa révélation ou ses conséquences<sup>92</sup>.

L'identification des enfants qui apparaissent sur les images abusives est d'autant plus délicate qu'il est capital de les protéger et de leur offrir un soutien psychosocial approprié. Les images peuvent circuler sur Internet pendant de nombreuses années ; par exemple, l'image d'une fillette de 5 ans peut toujours être en ligne 20 ans plus tard. Pour contribuer à l'identification des victimes, INTERPOL (Organisation internationale de police criminelle) et plusieurs services nationaux chargés de l'application des lois ont élaboré des bases de données d'images abusives d'enfants. Un logiciel sophistiqué d'analyse d'images aide la police à évaluer si une image d'enfant contenue, par exemple, dans une collection qui vient d'être saisie, est identique à d'autres déjà découvertes par les services chargés de l'application des lois et incluses dans une base de données d'images connues. Le logiciel offre une application capable d'identifier les enfants maltraités pendant de longues périodes et dont l'aspect physique a dû changer au fur et à mesure qu'ils grandissaient. La démarche est importante à la fois pour constituer un dossier complet contre un suspect et pour déterminer la durée et la nature des abus subis par un enfant tout en le soutenant dans son rétablissement.

Les bases de données de photos de victimes sont des ressources précieuses. Elles permettent aux fonctionnaires de police de gagner un temps considérable et leur évite de visionner toutes les images. Ce dernier aspect est particulièrement important. Jusqu'à il y a peu, le travail de la police nécessitait souvent le visionnement répété d'images. À présent, une nouvelle technologie permet de réduire les images photographiques à un code numérique, ou « code de hachage », qui peut ensuite être utilisé pour suivre, retrouver et comparer les images, sans qu'un policier ne doive afficher l'image réelle<sup>93</sup>. Le Rapporteur spécial des Nations Unies sur la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants a souligné la nécessité de mettre en place des politiques éthiques explicites qui clarifient, d'une part, la manière dont les images sont utilisées, qui y a accès et dans quelles circonstances, et, d'autre part, les droits des victimes à l'information, c'est-àdire où et comment les images sont stockées94. Les unités de police et les permanences téléphoniques qui gèrent les images d'abus d'enfants établissent en général des protocoles qui régissent le temps et les emplacements de visionnement et de stockage des images. La nature très pénible des images peut s'avérer problématique pour les personnes qui s'en occupent. Il n'est pas rare que des services d'assistance psychologique soient proposés aux policiers et au personnel qui

travaillent dans les permanences téléphoniques où le visionnement d'images abusives est indissociable de leurs fonctions.

Internet est généralement perçu comme offrant aux utilisateurs - y compris aux éventuels délinquants un anonymat qui permet de construire des identités et de décider à quel moment, comment et dans quelle mesure ils souhaitent publier des informations personnelles dans l'environnement en ligne<sup>95</sup>. En agissant de la sorte, leur identité ou les informations personnelles identifiables demeurent privées. Cet anonymat présumé crée un sentiment de sécurité et de confidentialité tant pour les délinquants que pour leurs victimes potentielles 96. Jadis, dans un contexte hors ligne, pour trouver des victimes, les pédoprédateurs se rendaient sur les aires de jeux, dans les associations et autres lieux publics où les enfants se rassemblaient. Aujourd'hui, le haut niveau d'interaction sociale en ligne pratiqué par les enfants fournit aux agresseurs un nouvel environnement pour cibler les enfants sans, pensent-ils à tort, courir les risques auxquels ils étaient confrontés auparavant, lorsque les contacts étaient directs (face à face).

Les enquêtes menées sur les activités criminelles en ligne sont complexes et fastidieuses. Souvent, elles nécessitent la coordination entre plusieurs juridictions et concernent un vaste réseau de délinguants. La mise en œuvre efficace de ces enquêtes achoppe sur un certain nombre de contraintes. Citons, en premier lieu, le manque d'expertise spécialisée. La lutte contre l'exploitation et les abus sexuels commis en ligne et hors ligne sur des enfants requiert une bonne connaissance des méthodes policières, de l'informatique, de la technologie d'Internet et de la protection des enfants. Dans de nombreux pays à revenu faible et intermédiaire, les unités spécialisées font cruellement défaut et le personnel est peu susceptible de recevoir la formation nécessaire pour enquêter sur la criminalité en ligne. Même si le personnel possède les compétences requises, la technologie pour enquêter sur ces délits n'est pas toujours disponible. Par conséquent, bien des services chargés de l'application des lois sont privés de moyens utiles pour la détection, l'instruction et les poursuites des crimes liés aux activités en ligne<sup>97</sup>.

Parmi les autres défis à relever, épinglons le manque de coordination et de collaboration entre les différents organismes. Pour les services chargés de l'application des lois, l'exploitation sexuelle en ligne n'est pas toujours une question de protection. En effet, dans de nombreux pays, l'exploitation sexuelle en ligne et hors ligne est qualifiée de « cybercriminalité ». Les unités de police spécialisées en criminalité informatique ou cybercriminalité se focalisent généralement sur la fraude et la criminalité organisée ; or, souvent, elles ne disposent que de peu ou pas d'expertise – voire d'intérêt professionnel – en matière de protection des enfants. Si les sites Web pédopornographiques

commerciaux sont, légitimement, associés à la criminalité organisée ou se retrouvent dans le collimateur de fonctionnaires de police habitués à lutter contre la fraude ou le terrorisme, une grande partie de l'échange d'images d'abus et de manipulation sexuels n'est pas classée dans cette catégorie. Il est important que la police fournisse une réponse centrée sur l'enfant, ce qui arrive rarement lorsqu'elle mène seule une enquête sur les abus et l'exploitation en ligne des enfants. La participation de spécialistes de la protection de l'enfant dans l'enquête, pratique recommandée par le Centre de protection contre l'exploitation des enfants en ligne (CEOP) au Royaume-Uni, garantit que le jeune bénéficie d'une protection adéquate et que son bien-être est pris en compte à chaque étape de l'enquête98.

On ne dispose que de peu de données factuelles sur la manière dont les professionnels de l'aide sociale répondent aux nouveaux défis en matière de protection des enfants dans les environnements en ligne et hors ligne. Deux rapports récents mettent en avant le manque de connaissances et de sensibilisation aux risques d'abus sur Internet parmi les travailleurs sociaux. Si ces deux rapports concernent l'Europe du Nord (Allemagne et Norvège), le modèle qu'ils identifient est reproductible ailleurs99. Les études suggèrent qu'en général, les professionnels qui entrent en contact avec les enfants - enseignants, infirmières de crèche et d'école, professionnels de la santé, policiers, travailleurs sociaux et conseillers/ psychothérapeutes - ne sont pas suffisamment conscients des risques d'abus liés aux nouvelles technologies. Si, par exemple, ces derniers s'inquiètent des changements de comportement d'un adolescent de 13 ans, il ne leur viendra pas à l'idée que l'enfant puisse être victime d'une agression en ligne et ils omettront de l'interroger sur ses activités sur Internet. De plus, ces professionnels ne sont pas toujours préparés ou capables d'entendre ce que les enfants ont à leur dire. Parmi les causes identifiées de ce manque d'écoute, citons l'absence de confiance professionnelle, la formation inadéquate, le stress au travail, les barrières émotionnelles, leurs valeurs, attitudes et croyances personnelles, le défaut de connaissance des problèmes et le manque de soutien. Sans perdre de vue l'importance capitale et croissante que les TIC revêtent pour les enfants dans le monde entier, ce manque de sensibilisation entraîne l'incapacité des professionnels à identifier et à étudier un contexte où les abus sont de plus en plus importants<sup>100</sup>.

Afin d'établir le tableau synoptique des services de réhabilitation et thérapeutiques dont disposent les enfants victimes d'abus ou d'exploitation en ligne, un sondage ad hoc a été mené parmi les professionnels et les chercheurs expérimentés dans le domaine, dans le cadre de la présente étude<sup>101</sup>. Dix des vingt pays invités à participer – Allemagne, Afrique du Sud, Australie, Bahreïn, Danemark, Fédération de Russie, Inde, Islande, Lettonie et

Royaume-Uni – y ont répondu et ont permis d'établir les conclusions suivantes :

- Dans certains pays, des directives séparées et distinctes sont adressées à la police et aux travailleurs sociaux; dans d'autres, seule la police bénéficie d'instructions. Dans certains pays, les directives existantes ne sont pas respectées ou sont obsolètes.
- Les membres du personnel des centres qui assurent des services d'aide aux enfants ayant subi un traumatisme indiquent qu'ils ne se sentent pas à l'aise pour travailler sur de tels cas.
- Six pays ont pu donner des exemples de collaboration entre les polices nationale et régionale et les travailleurs sociaux, dont des enquêtes spécifiques et des lignes d'assistance téléphonique.
- Neuf des dix pays consultés n'ont pas de système national permettant d'enregistrer le nombre et la nature des délits commis contre les enfants sur Internet. Dans certains pays, des informations partielles proviennent de certaines sources comme les services d'assistance téléphonique, le CEOP et les services d'aide ad hoc. L'Islande, quant à elle, constitue une exception. Ce pays possède un point d'appel centralisé permettant la redirection des appels liés à la protection des enfants. Sous le nom de Kinder House (maison des enfants), il offre un service universel à tous les enfants victimes dans le pays et propose un modèle multidisciplinaire de collaboration avec la police, les travailleurs sociaux, les avocats et les conseillers.
- Quatre des répondants ont déclaré qu'il n'y avait aucun exemple de participation de leur pays à des enquêtes internationales; un autre ignorait s'il y en avait et les cinq derniers ont décrit des opérations internationales complexes ayant duré plusieurs mois et impliqué un certain nombre de pays et qui ont abouti à la protection des enfants et à la condamnation des auteurs des abus.
- Le Bahreïn, dont la réponse stratégique aux crimes commis en ligne contre les enfants est minime, a signalé avoir réalisé, en 2010, un rapport concernant la sécurité sur Internet dans le pays. Outre l'analyse exhaustive des questions de sécurité sur Internet pour les adultes et les enfants, cet exercice formule des recommandations sur la sécurité des enfants sur Internet.

Bien que cette enquête n'ait qu'une portée limitée et ait été menée spécifiquement aux fins du présent rapport, ces résultats révèlent un panorama mitigé. Si les bonnes pratiques existent, il est cependant essentiel, pour assurer la protection efficace des enfants, de mettre en place des procédures plus systématiques et coordonnées par les

différents gouvernements et impliquant tous les organismes compétents.

### Un cadre de réponse

À la lumière des avantages majeurs apportés par Internet et les technologies connexes, de leur immense potentiel de transformation des vies, de la façon dont ils sont devenus incontournables dans nos sociétés modernes et font aujourd'hui partie intégrante du paysage social des jeunes, ce rapport propose un cadre stratégique pour la protection qui s'articule autour de quatre objectifs principaux :

### 1. Autonomiser les enfants et renforcer leur résilience face aux préjudices

La majorité des articles de presse dénonçant la criminalité en ligne ont tendance à dépeindre les enfants et les jeunes, particulièrement les filles, comme des victimes réelles ou potentielles n'ayant que peu de capacité d'agir. En ce qui concerne les images abusives d'enfants publiées en ligne, où apparaissent généralement des mineurs de moins de 10 ans, le consentement ou les capacités n'ont que peu d'incidence sur le fait qu'ils sont exposés à un danger. Pourtant, des études menées un peu partout dans le monde indiquent qu'en matière de manipulation en ligne ou de cyber-harcèlement, la capacité d'agir est un facteur essentiel.

En matière de manipulation, l'expérimentation, l'exploration et l'intérêt dont les jeunes font preuve pour se définir eux-mêmes socialement et sexuellement sont autant de facteurs de risque. À l'inverse, l'orientation exploratoire des jeunes leur permet d'accéder aux nombreux avantages d'Internet en termes d'éducation, de culture et de créativité. Par conséquent, les activités de prévention et de protection doivent tenir compte de la mesure dans laquelle la participation des enfants à la communication en ligne les engage dans des comportements potentiellement à risque tout en jouant un rôle capital dans la construction de leur identité, dans l'élaboration d'un réseau d'autoefficacité et de relations humaines, au sein d'un espace social dont les jeunes ont pris possession.

La participation active des enfants et des jeunes à l'élaboration et la mise en œuvre des mesures de protection donnera lieu à des stratégies qu'ils comprendront et qui auront donc toutes les chances d'être efficaces. Veiller à ce qu'ils disposent de l'information la plus pertinente possible sur la nature des risques associés aux activités en ligne, leur permettre de prendre les mesures nécessaires pour prévenir l'exposition à ces dangers et leur fournir le soutien nécessaire auprès d'adultes qui comptent dans leur vie sont autant d'éléments essentiels. Les enfants et les jeunes ont besoin de savoir à qui demander de l'aide, tout en reconnaissant qu'ils sont, eux-mêmes, une source primordiale

d'une grande partie de cette aide. Ils ont besoin de possibilités et de moyens pour signaler les activités ou les comportements inadmissibles, pour se faire éventuellement conseiller et pour avoir confiance non seulement dans les mesures prises suite à l'abus ou au préjudice mais aussi dans le fait qu'ils seront respectés comme des agents actifs. À cet effet, il y aura lieu de :

- Fournir aux enfants des informations qui leur permettent d'opérer un choix éclairé, d'éviter les risques, de trouver et d'offrir de l'aide en cas de nécessité. Plusieurs pays ont développé, pour établir une communication avec les enfants, des instruments innovants adaptables à différents contextes nationaux. SaferNet Brasil, par exemple, a créé une trousse éducative sur la sécurité en ligne conçue pour les enseignants dans le but d'améliorer la sécurité de leurs élèves sur Internet<sup>102</sup>. En République bolivarienne du Venezuela, le groupe Manos por la Niñez y Adolescencia (Mains pour les enfants et les adolescents) soutient la sécurité en ligne des enfants, adolescents, adultes et propriétaires de cybercafés.
- Mettre en œuvre des mécanismes de signalement efficaces, tels que les permanences téléphoniques, des fonctions de rapport d'abus et des aides en ligne pour anticiper les situations abusives. Sur certains sites de réseautage social, une icône sur la page d'accueil permet aux enfants interpellés par le comportement d'une personne qui communique avec eux de partager, en un seul clic, leurs inquiétudes et d'entrer immédiatement en contact avec les services chargés de l'application des lois.
- Renforcer la capacité des parents à protéger leurs enfants par le biais de programmes qui les informent des avantages et des risques liés aux TIC, des stratégies que les enfants et les jeunes peuvent mettre en œuvre pour assurer leur sécurité, des ressources d'aide potentielles et de l'importance d'établir le dialogue avec leurs enfants et de soutenir ceux-ci.
- Renforcer les capacités des professionnels qui travaillent avec les enfants afin de les avertir des risques encourus par ceux-ci et de leur apprendre à reconnaître les symptômes et les signes avant-coureurs. En Thaïlande, par exemple, une initiative numérique d'alphabétisation sur l'utilisation d'Internet en toute sécurité a débouché sur un module de formation qui a servi à former quelque 300 enseignants. Ces derniers ont ensuite communiqué ces messages de sécurité à plus de 70 000 enfants<sup>103</sup>.
- Impliquer les enfants en qualité de militants et défenseurs et utiliser leurs points de vue et leurs expériences propres pour élaborer une protection plus efficace. En Afrique du Sud, au Bénin, en Gambie, au Kenya, au Mozambique, au Nigéria

et au Togo, les jeunes ont créé, avec le soutien de l'ECPAT, des campagnes de sensibilisation sur les risques liés à l'environnement en ligne et sur la responsabilité des gouvernements et des fournisseurs de TIC en matière d'amélioration de la protection des enfants en ligne 104.

Faire face au cyber-harcèlement grâce à l'élaboration d'initiatives qui mettent en place la tolérance zéro vis-à-vis de la violence et des abus dans les écoles, ainsi que dans le cyberespace, et qui créent des mesures éducatives fondées sur les principes de l'acceptation, du respect et de la décence partagés par les élèves¹05. En Croatie, par exemple, une campagne nationale contre le cyberharcèlement a débouché sur des changements importants dans les écoles et la diminution de la violence.

#### 2. Mettre fin à l'impunité des abuseurs

Tant que les abuseurs s'estimeront à l'abri des poursuites et de la réprobation sociale, ils continueront d'exploiter ou de maltraiter les enfants. Il est donc indispensable de mettre fin à l'impunité de ceux qui persistent à commettre ces actes dans les environnements en ligne et hors ligne fusionnés.

L'abus et l'exploitation sexuels des enfants commis en ligne sont un problème d'ordre mondial dont la prise en charge efficace exige une action coordonnée à tous les niveaux : national, régional et mondial. Sans cet engagement, les auteurs d'abus risquent de concentrer leurs efforts sur les pays où la protection des enfants est la plus faible et où ils pensent que l'exploitation est plus facile à commettre ou moins susceptible d'être découverte et poursuivie. L'élaboration d'une approche commune entre les différentes juridictions est capitale car elle permet d'apporter une cohérence à la qualification et à la sanction pénales, de sensibiliser le public au problème, d'améliorer les services d'aide à la disposition des enfants victimes et de renforcer les efforts d'application des lois globale aux niveaux national et international<sup>106</sup>.

Compte tenu des disparités considérables entre les cadres juridiques existant dans les différentes régions du monde, la protection des enfants contre les abus en ligne et la poursuite des abuseurs présentent un défi de taille. La promulgation de lois destinées à protéger les enfants dans les environnements en ligne/hors ligne fusionnés s'avère complexe. La mise en place d'une démarche globale et cohérente rend la tâche encore plus difficile. La construction d'un environnement qui remette en question le rapport « coûts/bénéfices » pour les abuseurs et mette fin à leur impunité nécessite une approche holistique. Ce type d'approche s'efforce de garantir la nature indissociable des droits de l'enfant tout en étant applicable mondialement, grâce à la mise en œuvre de normes internationales pertinentes

et à la promotion de la collaboration et de la communication entre les gouvernements.

Les approches fondamentales suivantes sont proposées pour structurer l'instauration du cadre législatif et d'application des lois indispensable pour mettre fin à l'impunité des abuseurs :

- Introduction d'une législation nationale efficace dans laquelle figurent les définitions claires de l'enfant, du consentement sexuel, de la pédopornographie et des images abusives d'enfants; criminalisation de l'exploitation sexuelle des enfants par des adultes, y compris la possession, le téléchargement ou la création d'images abusives d'enfants, la manipulation, l'abus sexuel sans contact et les tentatives criminelles; sanctions et peines efficaces et adoption de mesures visant à relever les défis posés par la compétence judiciaire et l'extradition.
- Adoption d'un large éventail de stratégies en matière d'application des lois, combinée à une étroite collaboration entre les organismes d'aide sociale et de protection de l'enfant, à des opérations sous couvert et à l'identification des victimes. Les travailleurs sociaux, les enseignants et les psychologues peuvent prodiguer de précieux conseils qui garantiront l'utilisation exclusive des techniques d'interrogatoire et d'enquête appropriées et aideront la police à se concentrer essentiellement sur la protection des victimes tout au long des poursuites judiciaires engagées à l'égard des auteurs. Certains pays, parmi lesquels l'Australie, le Canada, les États-Unis, la Nouvelle-Zélande et le Royaume-Uni, qui travaillent ensemble dans le cadre de la Virtual Global Taskforce, ont mis en place des unités spécialisées qui se focalisent sur la poursuite judiciaire de l'exploitation et des abus sexuels dont sont victimes les enfants en ligne, tout en permettant la collaboration de différents professionnels.
- Coopération avec les fournisseurs d'accès à Internet, l'industrie des paiements en ligne et les autres intervenants du secteur privé afin de traquer les abuseurs sexuels sur des enfants et de fermer les voies d'accès à ces types de crimes. Voici quelques exemples : la Financial Coalition against Child Pornography, mise en place par le National Center for Missing & Exploited Children aux États-Unis et financée, entre autres, par des banques ; la Coalition européenne de partenaires contre l'exploitation sexuelle des enfants à des fins commerciales sur Internet, initialement dirigée par le CEOP et soutenue par MasterCard et Visa. En 2009, la Financial Coalition états-unienne a lancé une initiative en Asie à laquelle se sont associées des banques et des institutions financières basées à Singapour. Microsoft a également établi un partenariat avec les services chargés de l'application des lois et les fournisseurs de services Internet dans plusieurs pays afin d'instaurer des initiatives visant à mettre

un terme à l'exploitation sexuelle des enfants sur Internet.

- Instauration de l'obligation de signalement pour les professionnels qui travaillent avec les enfants sur les abus présumés, tout en gardant à l'esprit que l'efficacité de cette déclaration dépend de la qualité des services disponibles pour donner suite aux rapports<sup>107</sup>. La déclaration obligatoire pourrait être étendue et inclure d'autres personnes susceptibles de découvrir des preuves d'abus sexuels en raison de leur profession (par exemple, les professionnels des TIC, les développeurs de photos et les sociétés d'entretien d'ordinateurs)<sup>108</sup>.
- Collaboration entre les services chargés de l'application des lois au niveau international et développement d'outils qui contribuent à recueillir des preuves dans les affaires criminelles et facilitent l'échange de données entre les services chargés de l'application des lois de tous les pays. Ainsi, INTERPOL (Organisation internationale de police criminelle) coordonne les enquêtes à grande échelle menées dans plusieurs pays membres et utilise un outil de répression efficace, la « notice verte », qui adresse à la communauté internationale des services chargés de l'application des lois des alertes relatives aux délinquants susceptibles de commettre des récidives dans d'autres pays<sup>109</sup>.
- Garantie que les enfants impliqués dans des infractions sexuelles en ligne ne seront pas tenus pour pénalement responsables. Les enfants doivent être reconnus comme victimes, qu'ils soient des victimes consentantes ou des témoins non coopératifs. Lorsque des enfants de moins de 18 ans ont participé à des abus sexuels ou de harcèlement en ligne et que leur comportement est jugé illégal, la réponse des États doit être donnée par le biais de la justice compétente pour les mineurs, en collaboration avec les systèmes de protection des enfants, plutôt que par le système judiciaire pénal, conformément aux normes internationales<sup>110</sup>.

### 3. Réduire la disponibilité et l'accès aux contenus nuisibles

Si l'objectif principal consiste à éradiquer l'exploitation et les abus sexuels commis en ligne et hors ligne sur les enfants, force est de constater qu'en réalité, des millions d'images abusives d'enfants continuent à être disponibles sur Internet et sont susceptibles d'y rester dans un avenir proche. Des stratégies sont nécessaires pour réduire le nombre d'images créées, stockées et diffusées, ainsi que pour limiter l'accès aux agresseurs potentiels et aux enfants susceptibles de rencontrer des sites nuisibles lorsqu'ils sont en ligne. La présence persistante d'images d'abus d'enfants encourage d'autres exploitations d'enfants, conduit à une augmentation du nombre d'agresseurs et entraîne

une exposition des enfants à des abus répétés et sans limites. L'intérêt supérieur des enfants doit être assuré en consentant le maximum d'efforts pour veiller à ce que leurs images soient rapidement supprimées de la circulation, que l'accès aux sites commerciaux soit bloqué et que des mécanismes soient introduits pour en limiter la disponibilité et l'accès.

Certains enfants continueront à adopter des comportements à risques sans tenir compte des informations reçues parce qu'ils sont curieux, qu'ils n'ont pas conscience des implications de leurs actes, tant sur le plan social qu'au niveau de la nature et des conséquences de la technologie, qu'ils ont la fausse impression de garder le contrôle et qu'ils pensent que ce sont les autres, et non eux-mêmes, qui courent des risques.

Comme précisé plus haut dans le présent rapport, l'industrie des TIC assume un important faisceau de responsabilités pour réduire ces risques. Si le leadership des sociétés impliquées est essentiel, l'action collective ne l'est pas moins. Pour enrayer la disponibilité des images abusives et réduire le préjudice, il est indispensable que s'établisse une collaboration étroite entre les gouvernements et les acteurs du secteur privé, y compris les FSI, les sites de réseautage social, les propriétaires de cybercafés et les services d'hébergement des sites. Les efforts conjoints doivent porter, notamment, sur :

- La mise au point de codes de conduite et de systèmes d'autorégulation. Ces derniers devraient déboucher sur un mécanisme par lequel les entreprises peuvent exprimer et respecter les critères liés aux droits de l'homme en adoptant de meilleures pratiques volontaires et nonobligatoires à titre de guide pour la direction et le personnel. La rédaction de codes de conduite fait naître des défis : en effet, les entreprises pourraient considérer le profit, les relations publiques et les droits de l'homme comme étant antagonistes. L'expérience du Royaume-Uni montre que les codes de conduite dissociés de moyens de surveillance efficaces et clairement indépendants n'obtiennent pas la confiance du public<sup>111</sup>. Un conflit d'intérêts peut survenir si les sociétés multinationales opèrent ellesmêmes la surveillance ou la confient à leurs sous-traitants. Sans la surveillance d'une tierce partie indépendante, l'entité commerciale n'est pas réellement incitée à observer les conditions énoncées par le code.
- À l'échelle locale, la promotion de codes de conduite dans les cybercafés afin d'encourager leurs propriétaires à introduire des mesures visant à éviter que les enfants qui utilisent leurs établissements ne soient exposés à des sites et des contenus inappropriés ou à des comportements abusifs (et imposer une responsabilité claire aux cafés qui manquent à leur devoir de protection des enfants).

- Le blocage des sites Internet qui contiennent des images abusives d'enfants afin d'en refuser l'accès aux agresseurs potentiels. Le blocage est controversé et fait craindre une censure plus large. Dans tous les cas, il ne s'agit que d'une mesure temporaire qui ne doit rester en place que jusqu'à ce que le matériel illégal soit retiré à la source<sup>112</sup>. Bien que les outils de blocage ne soient pas toujours considérés comme efficaces (les images sont anciennes, l'utilisation des petites zones protégées d'Internet a augmenté, le contenu illégal peut être hébergé dans différents pays), les mesures de blocage restent nécessaires pour cibler le matériel pédopornographique.
- Le retrait de sites afin d'éliminer les images abusives d'Internet, mieux connu sous le nom de « procédures de notification et de retrait »<sup>113</sup>. Une fois identifié et signalé, tout site ou contenu comprenant des images abusives d'enfants est notifié au FSI qui l'héberge avec injonction de retirer le contenu illégal. La gestion des activités abusives sur ces sites constitue un réel défi, vu le volume des contenus concernés. Les procédures de notification et de retrait se sont avérées efficaces dans certains pays, notamment au sein de l'Union européenne<sup>114</sup>. Toutefois, et en dépit du fait que les images abusives d'enfants sont illégales dans la majorité des juridictions - ce qui peut sembler faciliter le retrait - leur élimination tend à être traitée avec moins de rapidité que les mesures prises à l'encontre d'autres types d'activités illégales sur Internet<sup>115</sup>. Le défi réside notamment dans l'inadéquation des ressources policières et dans la priorité donnée à la poursuite des délinquants plutôt qu'à l'adoption de mesures préventives comme le retrait des sites.
- Parallèlement aux images abusives d'enfants, il y a lieu également d'instaurer un ensemble plus vaste de mesures de protection des enfants, comme la mise au point de mesures de sécurité cohérentes, conviviales et facultatives dans les forums interactifs comme les salons de discussion ou les SRS et de veiller à ce que la position par défaut des paramètres de sécurité soit la nonparticipation plutôt que la participation.
- Les filtres et autres types de logiciels de contrôle parental permettent aux parents de gérer et de faciliter l'accès de leurs enfants à la toile. Cependant, des données factuelles ont montré que, malgré cette disponibilité, seule un peu plus de la moitié des parents active le logiciel de filtrage sur leurs ordinateurs<sup>116</sup>. Certains pensent qu'il est activé automatiquement, tandis que d'autres croient que leurs enfants arrivent à esquiver les contrôles. À Hong Kong, par exemple, le Council of Social Service attire l'attention sur les moyens efficaces d'utiliser les logiciels et les services de filtrage en ligne en fournissant des services de filtrage gratuits et en formant les parents à leur utilisation.

Des mesures simples, comme s'assurer que le navigateur web est en mode de « recherche sécurisée », peuvent fournir aux enfants une protection supplémentaire, mais très peu de parents semblent connaître la démarche à suivre. Le défi à relever par les communautés de gestion des moteurs de recherche consiste à déterminer s'il faut installer la recherche sécurisée par défaut sur tous les navigateurs ou expliquer beaucoup plus clairement la manière de la lancer sur tous les ordinateurs, en particulier ceux utilisés par les enfants.

# 4. Favoriser la réadaptation des enfants menacés

En dépit des mécanismes législatifs, politiques et de protection visant à prévenir l'exploitation et les abus sexuels, il ne fait aucun doute que certains enfants ont déjà subi des préjudices et que d'autres en subiront encore dans le monde en constante évolution du cyberespace et dans son interface avec l'environnement hors ligne. La recherche sur les stratégies efficaces pour minimiser l'impact et soutenir la réadaptation et la réhabilitation des enfants dans ce contexte n'en est encore qu'à ses balbutiements. Les données disponibles aujourd'hui ont été récoltées presque exclusivement dans le monde industrialisé. Pourtant, nous disposons de suffisamment de connaissances relatives à l'incidence des abus en ligne et à leurs liens avec les expériences hors ligne des enfants pour identifier les stratégies clés nécessaires afin de fournir à ces derniers le soutien psychosocial nécessaire. Si le chemin d'accès aux abus peut être particulier, les bonnes pratiques nécessiteront d'intégrer la dimension d'Internet dans les systèmes de réadaptation qui traitent des abus de façon plus générale, plutôt que de créer des services spécialisés. Il y a lieu de :

 Mettre en place des interventions thérapeutiques pour les enfants victimes d'abus en vue de restaurer la confiance et de leur apporter le soutien et l'aide nécessaires pour qu'ils puissent donner un sens à leur expérience. Certains enfants victimes de manipulation en ligne se sentent honteux d'avoir été « dupés » dans la relation en ligne qu'ils ont entretenue avec un adulte abuseur. D'autres se considèrent comme jouissant de suffisamment d'autonomie et de contrôle et ne se reconnaissent pas comme des victimes ayant besoin d'aide<sup>117</sup>. La plupart des enfants abusés par une manipulation en ligne se débattent au sein d'une dynamique conflictuelle – ils se perçoivent comme agissant comme un adulte en ligne, mais, hors ligne, ils continuent à jouer le rôle d'enfant ou de jeune<sup>118</sup>. Il est également capital d'apporter une aide aux parents de manière à ce qu'ils puissent comprendre les expériences en ligne de leurs enfants et leur offrir un soutien.

- Instaurer des approches spécifiques à l'enfant lors des enquêtes criminelles afin de prendre en compte les difficultés profondes que ressentent souvent les enfants et les jeunes au moment de révéler les abus en ligne. Il est important, par exemple, de veiller à respecter le minutage et le rythme adaptés pendant les interrogatoires, à éviter la répétition des témoignages en les enregistrant et à aider l'enfant à retrouver la capacité d'agir et le contrôle dont il a été privé pendant sa malheureuse expérience. En réponse à la nécessité de protéger les enfants victimes d'abus d'un nouveau traumatisme pendant l'enquête, certains pays comme le Canada, les États-Unis, l'Islande et le Royaume-Uni ont mis en place des centres de services intégrés. Des professionnels formés en techniques policières, santé mentale, défense des victimes et soins de santé y travaillent de concert pour collecter des informations judiciaires et prévenir de nouveaux traumatismes 119.
- Préparer la comparution devant un tribunal pour s'assurer que les enfants comprennent la procédure, leur rôle au cours de celle-ci, le soutien sur lequel ils peuvent compter et la manière de protéger leur confidentialité, tout en leur offrant la possibilité de comptesrendus et de conseils au cas où le passage au tribunal s'avèrerait difficile 120.
- Organiser un traitement destiné aux jeunes qui affichent des comportements d'abus sexuels en ligne. Ce traitement doit trouver son origine dans les mêmes approches que celles appliquées aux auteurs d'actes sexuels préjudiciables hors ligne. Il doit inclure l'évaluation complète de l'enfant et d'une intervention efficace, grâce à la réhabilitation et au conseil, l'évaluation du développement et de la motivation de l'enfant et l'implication active de ses parents dans le processus.



### CONCLUSION

Le puissant impact qu'exerce Internet sur la vie des enfants du monde entier ne cesse de croître et d'évoluer. Si l'accès à Internet et son utilisation par les enfants sont plus élevés dans les pays industrialisés, le rythme mondial d'accès à la toile et de pénétration du haut débit, ainsi que la courbe exponentielle du développement des technologies de téléphonie mobile, assortis à la croissance des capacités et à la diminution des coûts permettent au reste du monde de rattraper son retard. Au cours des prochaines années, on prévoit que l'évolution la plus marquée se produira dans les pays à revenu faible et intermédiaire.

Aujourd'hui, la plupart des données factuelles liées à certains types d'abus sont issues du monde industrialisé. Parallèlement, la majorité des résultats d'enquête sur les manières dont les jeunes utilisent Internet et les technologies associées, ainsi que les risques qu'ils courent, émane des mêmes régions. Pourtant, même à ce niveau, les connaissances restent très lacunaires. On ne dispose que de peu d'informations, par exemple, sur l'utilisation d'Internet par les enfants handicapés, sur le cyber-harcèlement et sur les défis auxquels sont confrontés les jeunes lesbiennes, gays, bisexuels et transgenres. Les connaissances lacunaires sur les risques et l'utilisation d'Internet en Afrique, ainsi que dans une grande partie de l'Asie et du Moyen-Orient, sont importants et doivent faire l'objet de recherches urgentes.

Toutefois, la recherche limitée menée dans les pays à revenu faible et intermédiaire montre que les questions soulevées dans le présent rapport sont pertinentes dans le monde entier ou sont sur le point de le devenir. Ainsi, les chercheurs ont acquis la certitude que les enfants de pratiquement tous les pays du monde utilisent les réseaux sociaux de manière très similaire et créent des occasions d'interactions aisées pour les éventuels manipulateurs. Les enfants originaires des pays à revenu faible et intermédiaire sont moins susceptibles d'utiliser Internet à partir de leur domicile et se rendent plutôt dans des cybercafés où ils courent un risque accru de voir des images inappropriées et d'être soumis à des sollicitations en ligne et hors ligne. Le manque de sensibilisation et de connaissances des parents, les conditions économiques difficiles et les cadres législatifs sous-développés peuvent exacerber davantage les dangers potentiels et la menace de préjudice. Ainsi, il s'avère que les lacunes constatées dans la protection des enfants et des jeunes dans l'environnement en ligne sont plus importantes dans les pays à revenu faible et

intermédiaire, où la protection globale des enfants est également défaillante.

À l'échelle mondiale, l'évolution de l'utilisation des TIC présente d'importants défis à relever. Seule une faible proportion d'adultes contemporains avait accès aux TIC lorsqu'ils étaient enfants, en particulier aux outils qui ont facilité la révolution de l'interaction et de la communication. Cette situation a probablement affecté la capacité des adultes à comprendre et à éprouver de l'empathie pour la manière dont les enfants et les jeunes utilisent Internet, les téléphones portables et les autres technologies modernes. Ceci est sans doute particulièrement vrai dans les sociétés où l'activité sociale des enfants, et en particulier des adolescents, est soumise à une surveillance ou un contrôle parental plutôt assidu. Cette situation devrait évoluer au fil du temps, au fur et à mesure que les jeunes d'aujourd'hui, rompus à l'informatique et aux réseaux sociaux, deviendront eux-mêmes parents. Sans doute, éprouveront-ils moins d'inquiétude quant au risque d'exploitation et d'abus car ils auront fait partie de la génération qui a développé les moyens de les gérer. En revanche, la créativité engendrée par les TIC est de nature à générer sans cesse de nouveaux éléments qui posent les jalons d'autres dangers auxquels il sera impératif de répondre par des stratégies novatrices.

Dans les endroits où leur accès est très répandu, les TIC ont, dans un laps de temps très court, révolutionné le mode de vie des individus et leurs relations mutuelles. Dans les lieux où l'accès est en pleine expansion, ces changements sont en cours. Il ne fait aucun doute que des évolutions considérables se produiront encore, mais il nous est impossible de dire à quoi elles ressembleront. Le cyberespace met en exergue les rôles sociaux et les responsabilités des acteurs au-delà des États, c'est-à-dire du secteur privé et des individus eux-mêmes. Il a le potentiel d'enrichir tant les individus que la société, de contribuer à supprimer les barrières entre les gens, d'ouvrir la voie à l'interaction, à l'éducation et au développement, mais il prête aussi le flanc aux actes répréhensibles. Or, les enfants sont au cœur de ce dilemme. Si les enfants et les jeunes sont indissociables de la construction d'un Internet plus sûr, c'est aux gouvernements et au secteur privé qu'il incombe de veiller, en promouvant l'élargissement de l'accès à Internet et ses avantages positifs, à intégrer cette protection.

## **RÉFÉRENCES**

- ONG Européenne Alliance for Child Safety Online (Alliance pour la sécurité des enfants en ligne), « The Right Click: An agenda for creating a safer and fairer online environment for every child », ONG Européennef Alliance for Child Safety Online, eNACSO, Copenhague, juin 2010, pp. 2, 5, 8, 17, disponible sur: <www.enacso.eu/images/stories/ Documents/manifesto/afafinal6may.pdf>, consulté le 22 août 2011.
- 2 Lobe, B., et al. (en collaboration avec les membres du réseau EU Kids Online), Cross-National Comparison of Risks and Safety on the internet: Initial analysis from the EU Kids Online survey of European children, EU Kids Online, London School of Economics and Political Science, Londres, août 2011, p. 13.
- 3 Assemblée générale des Nations Unies, Rapport du Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie, Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, A/HRC/17/31, Nations Unies, New York, 21 mars 2011, Principes directeurs 11 et 13 (b).
- 4 Livingstone, S., et al., Risks and Safety on the Internet: The perspective of European children, Full Findings and policy implications from the EU Kids Online survey of 9–16 year olds and their parents in 25 countries, EU Kids Online, London School of Economics and Political Science, Londres, 2011.
- 5 Livingstone, S. et L. Haddon, EU Kids Online: Final report, EU Kids Online, London School of Economics and Political Science, Londres (EC Safer Internet Plus Programme Deliverable D6.5), juin 2009. L'étude a porté sur 21 pays européens : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, France, Grèce, Islande, Irlande, Italie, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Slovénie, Suède et Royaume-Uni.
- 6 Carr, J. et Z. Hilton, *Digital Manifesto*, Children's Charities Coalition on Internet Safety, Londres, 2009, p. 29.
- 7 Carr, J., « Briefing Note on Child Abuse Images and the Internet », Children's Charities Coalition on Internet Safety, Londres, juillet 2010, p. 2.
- 8 Internet Watch Foundation, Annual and Charity Report 2010, IWF, Londres, 2010, p. 1; Quayle, E. et T. Jones, « Sexualised images of children on the internet, Sexual Abuse », vol. 23, n° 1, mars 2011, pp. 7–21.
- 9 Voir par exemple: Bureau de l'ombudsman fédéral des victimes d'actes criminels [Canada], Chaque image, chaque enfant: L'exploitation sexuelle d'enfants facilitée par Internet au Canada, Ministère de la Justice, Gouvernement du Canada, 2009, p. 8, disponible sur: <www.victimesdabord.gc.ca/ pdf/pjuvenile-childp.pdf>; Wolok, J., D. Finkelhor

- et K. J. Mitchell, *Child Pornography Possessors*Arrested in Internet Related Crimes: Findings from the National Juvenile Online Victimization Study,
  National Center for Missing and Exploited Children,
  Alexandria, Virginie, 2005, pp. vii, 5, 6.
- 0 Internet Watch Foundation, Annual and Charity Report 2010, IWF, Londres, 2010, disponible sur: <www.iwf.org.uk/accountability/annualreports/2010-annual-report>; Internet Watch Foundation, Annual and Charity Report 2006, IWF, Londres, 2006, p. 8, <www.enough.org/ objects/20070412\_iwf\_annual\_report\_2006\_web. pdf>.
- 11 Internet Watch Foundation, *Annual and Charity Report 2010*, p. 8.
- 12 Baines, Victoria, « Online Child Sexual Abuse: The law enforcement response – A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents », ECPAT International, Bangkok, novembre 2008, p. 2.
- 13 Webster, S., et al., Scoping Report: European Online Grooming Project, Projet European Online Grooming dans le cadre du programme de la Commission européenne « Pour un Internet plus sûr », Londres, avril 2010, p. 7. Le rapport définit les jeunes comme étant toute personne de moins de 16 ans.
- 14 Mitchell, Kimberly J., et al., « Use of Social Networking Sites in Online Sex Crimes Against Minors: An examination of national incidence and means of utilization », Journal of Adolescent Health, vol. 47, n° 2, août 2010, pp. 183–190.
- 15 Webster, S., et al., Scoping Report: European Online Grooming Project, p. 13.
- 16 Ethel Quayle, « Sexualized Images of Children on the Internet », *Sexual Abuse*, vol. 23, n° 1, mars 2011, pp. 7–21.
- 17 Wolak, J., et al., « Online "Predators" and their Victims: Myths, realities and implications for prevention and treatment », American Psychologist, vol. 63, n° 2, février-mars 2008, pp. 111–128, disponible à l'adresse <www.apa.org/pubs/journals/releases/amp-632111.pdf>.
- Voir par exemple: Wolak, J., D. Finkelhor et K. J. Mitchell, Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study, National Center for Missing and Exploited Children, Alexandria, Virg., 2005, disponible sur: <www. missingkids.com/en\_US/publications/NC144. pdf>; Sullivan, C., « Internet Traders of Child Pornography: Profiling research », New Zealand Department of Internal Affairs, Wellington, 2005; Webb, L., J. Craissati et S. Keen, « Characteristics of Internet Child Pornography Offenders: A comparison with child molesters », Sex Abuse, vol. 19, 16 novembre 2007, pp. 449-465; Bates A., et C.A. Metcalf, « A Psychometric Comparison of Internet and Non-Internet Sex Offenders from a Community Treatment Sample », Journal

- of Sexual Aggression, vol. 13, n°1, mars 2007, pp. 11–20; Baartz, D., « Australians, the Internet and Technology-Enabled Child Sex Abuse: A statistical profile », Australian Federal Police, Canberra, Australie, 2008; Quayle, E., L. Loof et T. Palmer, « Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents », ECPAT International, Bangkok, novembre 2008.
- Voir par exemple: Wolak, J., K. Mitchell et D. Finkelhor, « Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users », Pediatrics, vol. 119, nº 2, février 2007, pp. 247-257, disponible sur : <a href="http://">http://</a> pediatrics.aappublications.org/content/119/2/247. full.pdf+html>; Mossige, S., M. Ainsaar et C. Göran Svedin, eds., The Baltic Sea Regional Study on Adolescents' Sexuality, NOVA, ministère norvégien de l'Éducation et de la Recherche, Oslo, 2007, p. 37; Soldatova, G., « Russian Schoolchildren as Internet Users: Types and risk groups », Foundation for Internet Development, 1999; Muhammad T., « Danger for children at Pakistan's cafes », Bulletin de l'ECPAT No 48, juillet 2004, p.5, citant Pakistan Paediatric Association et Save the Children Suède, Exposure of children to pornography at Internet cafes of Pakistan, 2001.
- Voir par exemple: Liao, Lih Mei, et S. M. Creighton, «Requests for Cosmetic Genitoplasty: How should healthcare providers respond? », BMJ, vol. 334, n°7603, 24 mai 2007, pp. 1090–1092; et Braun, V. et L. Tiefer, «The "Designer Vagina" and the Pathologisation of Female Genital Diversity: Interventions for change », Radical Psychology, vol. 8, n°1, 2010, n.d.
- Voir par exemple: Lo, Ven-Hwei, et Ran Wei, « Exposure to Internet Pornography and Taiwanese Adolescents' Sexual Attitudes and Behaviour », Journal of Broadcasting & Electronic Media, vol. 49, n°2, juin 2005, pp. 221-237; Livingstone, S., et al., Risks and safety on the internet, Full findings, 2011 2011; CWIN Népal, « Protecting Children in Cyberspace », Katmandou, 2009, : disponible à l'adresse <www.nta.gov.np/articleimages/file/ Protecting%20Children%20in%20Cyberspace%20 WTIS.pdf>, 21 août 2011; Rauniar, Deepak, « Cyber Cafes of Nepal: Passage to cyber crime? », South Asia Partnership International et Bellanet Asia, Lalitpur, Népal, mars 2007; Chetty, lyavar, et Antoinette Basson, « Report on Internet Usage and the Exposure of Pornography to Learners in South African Schools », Film and Publication Board, Houghton, Afrique du Sud, novembre 2008.
- 22 Voir par exemple: Cross, D. et al., Australian Covert Bullying Prevalence Study (ACBPS), Child Health Promotion Research Centre, Edith Cowan University, Perth, Australie; Livingstone, S., et al., Risks and safety on the internet, Full findings 2011; SaferNet Brasil Surveys 2009, disponible sur: <www.safernet.org.br/site/prevencao/pesquisas>; Davidson, Julia, State of the Nation Review of Internet Safety 2010, Telecommunications Regulatory Authority, Royaume du Bahrein, Manama, 2010; Shariff, Shaheen, Cyber-Bullying: Issues and solutions for the school, the classroom and the home, Routledge, Londres et New York, 2008; National Children's Home and Tesco Mobile, « Putting U in the Picture: Mobile bullying survey 2005 », NCH, n.d.

- 23 Voir par exemple: Shariff, S., Cyber-Bullying: Issues and solutions for the school, the classroom and the home, Routledge, Londres et New York, 2008.
- 24 Livingstone, S., et al., Risks and safety on the internet, Full findings 2011.
- 25 Voir: Sharif, Shaheen, Cyber-Bullying.
- 26 Voir par exemple: Keith, Susan, et Michelle E. Martin, « Cyber-Bullying; Creating a culture of respect in a cyber world », Reclaiming Children and Youth, vol. 13, n°4, hiver 2005, pp. 224–228; et Sharif, Shaheen, Cyber-Bullying.
- 27 Raskauskas, Juliana, and Ann D. Stoltz, « Involvement in Traditional and Electronic Bullying among Adolescents », *Developmental Psychology*, vol. 43, n°3, mai 2007, pp. 564–575.
- 28 Voir par exemple: Hasebrink, U., et al., Patterns of risk and safety online: In-depth analyses from the EU Kids Online survey of 9–16-year olds and their parents in 25 countries. London School of Economics and Political Science, Londres; EU Kids Online, août 2011, pp. 7, 22, 31.
- 29 Union internationale des télécommunications, « Use of Information and Communication Technology by the World's Children and Youth: A statistical compilation », UIT, Genève, juin 2008; Lenhart, A., et al., « Social Media & Mobile Internet Use Among Teens and Young Adults », Pew Internet & American Life Project, Washington, D.C., 2010.
- 30 Livingstone, S. et L. Haddon, *EU Kids Online: Final report 2009*, p. 5.
- 31 Livingstone, S. et al, Risks and Safety on the Internet, Full findings, p. 31.
- 32 Union internationale des télécommunications, « Use of Information and Communication Technology by the World's Children and Youth »; Livingstone, S. et L. Haddon, EU Kids Online: Final report 2009.
- 33 Programme pour un Internet plus sûr, Eurobaromètre, Towards a safer use of the Internet for children in the EU – A parents' perspective, Eurobaromètre, Commission européenne, Bruxelles, décembre 2008, p. 13.
- 34 Livingstone, S. et al, Risks and Safety on the Internet, Full findings, p. 26.
- 35 Davidson, J. and E. Martellozzo, State of the Nation Review of Internet Safety 2010, Autorité de regulation des télécommunications, Royaume du Bahreïn, Manama, 2010, disponible à l'adresse <www.tra.org.bh/en/pdf/SafeSurf\_TRA\_Report. pdf>, 7 septembre 2011.
- 36 Chetty, Iyavar, et Antoinette Basson, « Report on Internet Usage and the Exposure of Pornography to Learners in South African Schools », Film and Publication Board, Houghton, Afrique du Sud, novembre 2008, p. 23.
- 37 Center of Studies on Information and Communication Technologies, « Survey on the Use of Information and Communication Technologies in Brazil 2009 », CETIC.br, Comité de gestion de l'Internet au Brésil, São Paolo, 2010, p. 227, disponible sur : <www.cetic.br/english/>. Ce pourcentage inclut les individus qui ont déclaré avoir eu accès à Internet au moins une fois dans leur vie à partir d'un endroit quelconque.
- 38 UIT, « Use of Information and Communication Technology by the World's Children and Youth », pp. 29, 41.
- Symantec, « Norton Online Living Report 09 », Mountain View, Californie, 2009, pp. intro, 4, 13, 14. Les pays sur lesquels porte l'étude sont

- l'Allemagne, l'Australie, le Brésil, le Canada, la Chine, les États-Unis, la France, l'Inde, l'Italie, le Japon, la Suède et le Royaume-Uni; l'étude est disponible sur <www.protegiendoles.org/documentacion/estante4/NOLR\_Report\_09.pdf>, consulté le 19 août 2011.
- 40 Union internationale des télécommunications, « The World in 2010: ICT facts and figures », UIT, Genève, 2010, pp. 4–5; disponible sur : <www. itu.int/ITU-D/ict/material/FactsFigures2010.pdf>, consulté le 26 août 2011.
- 41 Centro de Estudos sobre as Tecnologias da Informação e da Comunicação, « Survey on the Use of Information and Communication Technologies in Brazil 2009 », CETIC.br, 2009, pp. 54, 133, 239; Centro de Estudos sobre as Tecnologias da Informação e da Comunicação, « Survey on the Use of Information and Communication Technologies in Brazil 2008 », CETIC.br, 2008, p. 228; Centro de Estudos sobre as Tecnologias da Informação e da Comunicação, « Survey on the Use of Information and Communication Technologies in Brazil 2006 », CETIC.br, 2006, p. 113.
- 42 Données fournies par la délégation japonaise à l'OCDE, Organisation pour la coopération et le développement économique, « The Protection of Children Online: Risks faced by children online and policies to protect them », OECD Digital Economy Papers, N° 179, Éditions de l'OCDE, Paris, mai 2011, p. 10 ; et Eurobaromètre 2008, tableaux annexes et section « survey details », Towards a safer use of the Internet for children in the EU A parents' perspective, rapport d'analyse, tableau 21b, p. 112.
- 43 UIT, « Use of Information and Communication Technology by the World's Children and Youth », 2008. Au chapitre 5, p. 19, le rapport mentionne les classifications suivantes: *Children* (enfant) désigne les individus âgés de 5 à 14 ans ou moins; et *Youth* (jeune) désigne les individus âgés de 15 à 24 ans.
- 44 Lenhart, A. et al., « Social Media & Mobile Internet Use Among Teens and Young Adults », Pew Internet & American Life Project, Washington, D.C., 2010, disponible sur : <a href="http://pewresearch.org/pubs/1484/social-media-mobile-internet-use-teens-millennials-fewer-blog">http://pewresearch.org/pubs/1484/social-media-mobile-internet-use-teens-millennials-fewer-blog</a>, consulté le 9 juin 2011.
- 45 Livingstone, S., et al., Risks and Safety on the Internet, Full findings, p. 5, disponible sur: <www2. cnrs.fr/sites/en/fichier/rapport\_english.pdf>, consulté le 12 octobre 2011.
- 46 Socialbakers.com, « India Facebook Statistics, Penetration, Demography », Socialbakers Ltd., <www.socialbakers.com/facebook-statistics/ india#chart-intervals>, consulté le 12 octobre 2011.
- 47 Socialbakers.com, « Brazil Facebook Statistics », Socialbakers Ltd., <www.socialbakers. com/facebook-statistics/brazil>, consulté le 12 octobre 2011.
- 48 Byron, T. Safer Children in a Digital World: The Report of the Byron Review, Department for Children, Schools and Families, Annesley, Royaume-Uni, mars 2008, disponible sur: <a href="http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20">http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20</a> world%20the%202008%20byron%20review.pdf>.
- 49 Voir par exemple: Davidson, J., E. Martellozzo et M. Lorenz, « Evaluation of CEOP ThinkUKnow

- Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge », Centre for Abuse & Trauma Studies, Kingston University, Londres, juillet 2009, disponible sur: <a href="http://cats-rp.org.uk/pdf%20files/Internet%20">http://cats-rp.org.uk/pdf%20files/Internet%20</a> safety%20report%204-2010.pdf>, consulté le 21 août 2011; Davidson, J. C. et E. Martellozzo, « Educating children about sexual abuse and evaluating the Metropolitan police safer surfing programme », Project Report, Metropolitan Police, Londres, 2004; Donath, J., et Boyd, D., « Public displays of connection », BT Technology Journal, vol. 22, N° 4, octobre 2004, pp. 71-82, disponible sur: <www.danah.org/papers/PublicDisplays. pdf>; et Centre de protection contre l'exploitation des enfants en ligne, « Understanding Online Social Network Services and Risks to Youth: Stakeholder perspectives - A preliminary report on the findings of the CEOP Centre's social network seminar series », Centre de protection contre l'exploitation des enfants en ligne, Londres, 2006.
- 50 Donath, J., et Boyd, D., « Public displays of connection ».
- 51 Voir par exemple: Davidson, J., E. Martellozzo et M. Lorenz, « Evaluation of CEOP ThinkUKnow Internet Safety Programme »; International Youth Advisory Congress (A CEOP led VGT initiative), « IYAC Children and Young Persons' Global Online Charter Supplementary Document », Child Exploitation and Online Protection (CEOP) Centre, Londres, 2008.
- 52 Lobe, B., et al. (en collaboration avec les membres du réseau EU Kids Online), Cross-National Comparison of Risks and Safety on the internet: Initial analysis from the EU Kids Online survey.
- 53 Voir par exemple: SaferNet Brasil Surveys, 2009; et Davidson, J., State of the Nation Review of Internet Safety 2010, p. 4.
- Voir par exemple: Van der Gaag, Nikki, Because I Am a Girl: The State of the World's Girls 2010 Digital and urban frontiers: Girls in a changing landscape, Plan International, Bruxelles, 2010, disponible sur: <a href="http://plan-international.org/girls/resources/digital-and-urban-frontiers-2010.php">http://plan-international.org/girls/resources/digital-and-urban-frontiers-2010.php</a>, consulté le 27 août 2011; SaferNet Brasil Surveys, 2009; Lenhart, A., et al., « Social Media & Mobile Internet Use Among Teens and Young Adults », Pew Internet & American Life Project, Washington, D.C., 2010, p. 8; CWIN Nepal, « Protecting Children in Cyberspace ».
- 55 Voir: Lenhart, A., « Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging », Pew Internet & American Life Project, Washington, D.C., 15 décembre 2009, disponible sur : <www.pewinternet.org/~/media//Files/Reports/2009/PIP\_Teens\_and\_Sexting.pdf>.
- 56 Lenhart, A., Teens and Sexting, et SaferNet Brasil Surveys, 2009.
- 57 Ybarra, M. L., et K. J. Mitchell, « How Risky Are Social Networking Sites?: A comparison of places online where youth sexual solicitation and harassment occurs », *Pediatrics*, vol. 121, n° 2, 1er février 2008, pp. e350–e357; disponible sur: <a href="http://pediatrics.aappublications.org/content/121/2/e350.full">http://pediatrics.aappublications.org/content/121/2/e350.full</a>, consulté le 26 août 2011; Ybarra, M.,L. *et al.*, « Internet Prevention Messages: Targeting the right online behaviors », *Archives of*

- Pediatric and Adolescent Medicine, vol. 161, n° 2, février 2007, pp. 138-145, disponible sur : <a href="http://archpedi.ama-assn.org/cgi/content/full/161/2/138">http://archpedi.ama-assn.org/cgi/content/full/161/2/138</a>>.
- 58 Optem, « Safer Internet for Children: Qualitative study in 29 European countries –Rapport de synthèse », Eurobaromètre, Bruxelles, mai 2007, disponible sur : <a href="http://ec.europa.eu/public\_opinion/archives/quali/ql\_safer\_internet\_summary.pdf">http://ec.europa.eu/public\_opinion/archives/quali/ql\_safer\_internet\_summary.pdf</a>>.
- 59 Ybarra, M.,L. *et al.*, « Internet Prevention Messages », pp. 138–145.
- 60 Voir par exemple: UNICEF Regional Office for West and Central Africa, « Promoting Synergies between Child Protection and Social Protection: West and Central Africa », Overseas Development Institute and United Nations Children's Fund, Londres et Dakar, 2009, disponible sur: <www.odi.org.uk/resources/details.asp?id=3477&title=child-protection-social-protection-west-central-africa>.
- 61 Mitchell K. J., D. Finkelhor and J. Wolak, « Risk factors for and impact of online sexual solicitation of youth », *The Journal of the American Medical Association*, vol. 285, n° 23, 20 juin 2001, pp. 3011–3014; Dawes, A., and A. Govender, « The Use of Children in Pornography in South Africa », Human Sciences Research Council, Pretoria, 2007, disponible sur: <www.hsrc.ac.za/Research\_Project-796.phtml>.
- 62 Livingstone, S., « e-Youth: (Future) policy implications Reflections on online risk, harm and vulnerability », Presentation at « e-Youth: balancing between opportunities and risks » (26–28 mai 2010, Anvers, Belgique), London School of Economics Research Online, Londres, juin 2010, disponible sur: <a href="http://eprints.lse.ac.uk/27849/">http://eprints.lse.ac.uk/27849/</a>>.
- 63 Van der Gaag, Nikki, Because I Am a Girl: The State of the World's Girls 2010.
- 64 Van der Gaag, Nikki, Because I Am a Girl: The State of the World's Girls 2010; Bawagan, Aleli, et Anjanette Saguisag, « The Role of the Private Sector, particularly ISPs and Internet Café Owners, as Active Partners in Protecting Children from Sexual Abuse and Exploitation in the Philippines: An on-going case study by UNICEF Philippines », UNICEF, Makati, Philippines, n.d., disponible sur: <www.unicef-irc.org/files/documents/d-3600-Working-with-internet-ser.pdf>, 21 août 2011; Plan India, « Girls in a Changing Landscape: Urban and digital frontiers The state of the girl child in India 2010 », New Delhi, septembre 2010.
- 65 Voir par exemple: Long Island Network of Community Services/BiasHELP,
  « STOPtechNObullying: LGBTQ Lesbian, gay, bisexual, transgender and questioning youth », Hauppauge, New York, 2011, disponible sur: <a href="http://stoptechnobullying.org/lgbtq.php">http://stoptechnobullying.org/lgbtq.php</a>, consulté le 22 août 2011>; et Shariff, Shaheen, Cyber-Bullying.
- 66 Understanding social networking services and risks to youth, Stakeholder perspectives, a preliminary report on the findings of the CEOP centre's social network seminar series, Centre de protection contre l'exploitation des enfants en ligne, Londres, 2006; SaferNet Brasil Surveys 2009. Disponible sur: <www.safernet.org.br/site/prevencao/pesquisas>.
- 67 Centre de protection contre l'exploitation des enfants en ligne, « Understanding Social

- Networking Services and Risks to Youth: Stakeholder perspectives – A preliminary report on the findings of the CEOP Centre's Social Network Seminar Series », CEOP, Londres, 2006, disponible sur: <www.ceop.police.uk/Documents/ socialnetwork\_serv\_report\_221206.pdf>.
- 'Staying Safe Survey 2009: Young people and parents' attitudes around Internet safety', Department for Children, Schools and Families, Government of the United Kingdom, Runcorn, Royaume-Uni, décembre 2009; Livingstone, S. and L. Haddon, EU Kids Online: Final report.
- 69 Livingstone, S. and L. Haddon, *EU Kids Online:* Final report.
- 70 Voir par exemple: Davidson, J., State of the Nation Review of Internet Safety 2010; Staksrud, E. et S. Livingstone, « Children and Online Risk: Powerless victims or resourceful participants? », Information, Communication & Society, vol. 12, n° 3, 2009, pp. 364–387; Gallup Organisation, « Towards a Safer Use of the Internet for Children in the EU » (Eurobaromètre), <a href="http://ec.europa.eu/public\_opinion/flash/fl\_248\_en.pdf">http://ec.europa.eu/public\_opinion/flash/fl\_248\_en.pdf</a>>.
- 71 'Staying Safe Survey 2009: Young people and parents' attitudes around Internet safety'; and Livingstone, S. et L. Haddon, *EU Kids Online:* Final report.
- 72 Cho, Chang-Hoan, et Hongsik John Cheon, « Children's Exposure to Negative Internet Content: Effects of family context », Journal of Broadcasting & Electronic Media, 1er décembre 2005, pp. 488– 509
- 73 *Voir*: Staksrud, E. et S. Livingstone, « Children and Online Risk ».
- 74 Voir par exemple: Voices of Youth, « Survey on Internet Use, 2010 » (internal document), Fonds des Nations Unies pour l'enfance, New York; Van der Gaag, Nikki, Because I Am a Girl: The State of the World's Girls 2010.
- 75 Voir: Davidson, J., E. Martellozzo et M. Lorenz, « Evaluation of CEOP ThinkUKnow Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge ».
- 76 Livingstone, S., et al., Risks and safety on the internet, Full findings 2011.
- 77 Pour un aperçu complet des cadres juridiques, voir: Newell, P., « Legal Frameworks for Combating Sexual Exploitation of Children », Centre de recherche Innocenti de l'UNICEF, Florence, 2008.
- 78 Troisième congrès mondial contre l'exploitation des enfants, « The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents », 2008, p. 6, disponible sur : <www.ecpat.net/WorldCongressIII/ PDF/Outcome/WCIII\_Outcome\_Document\_Final. pdf>, consulté le 7 septembre 2011.
- 79 Nations Unies, Rapport de l'expert indépendant chargé de l'étude des Nations Unies sur la violence à l'encontre des enfants A/61/299, Assemblée générale des Nations Unies, New York, 29 août 2006, p. 32, paragraphe 114 (j),(k).
- 80 International Centre for Missing and Exploited Children, « Child Pornography: Model legislation & global review », 6th ed., ICMEC, Alexandria, Virg., 2010. Information disponible sur: <www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en\_X1&PageId=4346>, 22 septembre 2011.

- 81 Commission européenne, « Proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision cadre 2004/68/JAI », Commission européenne, Bruxelles, 29 mars 2010, disponible à l'adresse : <a href="http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107">http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107>
- Union européenne, Actes législatifs et autres instruments - Directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, Union européenne, Bruxelles, 4 novembre 2011. Voir également : Conseil de l'Union européenne, « L'UE prend des mesures pour lutter contre les abus sexuels concernant des enfants et contre la pédopornographie », Communiqué de presse, Conseil de l'Union européenne, Bruxelles, 15 novembre 2011. Disponible à l'adresse : < http://europa.eu/rapid/ pressReleasesAction.do?reference=PRES/11/428&f ormat=HTML&aged=0&language=FR&guiLangua ge=fr>
- GSMA, Mobilising Europe's Digital Agenda, GSMA, Londres, 2010, disponible sur: <www.gsmworld. com/our-work/public-policy/gsma\_europe/mobilising/downloads/GSMA\_UmbrellaStory\_A5Brochure.pdf>; GSM World, EuropeanFramework (page web), voir: <www.gsmworld.com/our-work/public-policy/framework\_mobile\_use\_younger\_teenagers\_children.htm>.
- 84 Donoso, V., Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 14 Social Networking Sites, Commission européenne, Programme « Pour un Internet plus sûr », Luxembourg, mai 2011, disponible à l'adresse: < :http://ec.europa.eu/information\_society/activities/social\_networking/eu\_action/implementation\_princip\_2011/index\_en.htm>. Voir également: Donoso, V., Assessment of the implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary report, Commission européenne, Programme « Pour un Internet plus sûr », Luxembourg, 2010.
- 'Mémorandum sur le droit à la protection des renseignements personnels et la vie privée dans les réseaux sociaux sur l'Internet, en particulier ceux des enfants et des adolescents', 2009, disponible en PDF dans les quatre langues suivantes, dans l'ordre suivant : en espagnol, portugais, anglais et français à l'adresse : <www.iijusticia.org/esp\_port\_eng\_fran.pdf>, consulté le 30 août 2011.
- 86 Gregorio, Carlos, « Sexual Abuse and Exploitation in the Converged Online/Offline Environment: A point of view from Latin America », document non publié; InSafe Annual Report 2010, InSafe Brussels, octobre 2010.
- 87 Voir par exemple: Wall, David S., « The Internet as a Conduit for Criminal Activity », Chapter 4 in April Pattavina, ed., Information Technology and the Criminal Justice System, Sage Publications, Thousand Oaks, CA, 2005, pp. 77–98, disponible sur: <a href="http://papers.ssrn.com/sol3/">http://papers.ssrn.com/sol3/</a>

- papers.cfm?abstract\_id=740626>, consulté le 7 septembre 2011.
- 88 Stephens, Gene, « Policing the Future: Law enforcement's new challenges », *The Futurist*, mars-avril 2005, pp. 51–57, <www.policefuturists. org/pdf/M-A2005Futurist\_Stephens>.
- 89 Palmer T., « Sexual abuse and exploitation in the converged online/offline environments: Referral services and rehabilitation » (document non publié du Centre de recherche Innocenti de l'UNICEF).
- 90 Voir par exemple: Palmer, Tink, « Behind the Screen: Children who are the subjects of abusive images », in Quayle, Ethel et Maxwell Taylor, eds., Viewing Child Pornography on the Internet: Understanding the offence, managing the offender, helping the victims, Russell House Publishing, Lyme Regis, UK, 2005; Palmer, T. et L. Stacey, Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology, Barnardo's, Ilford, UK, 2004; Julia Von WeilerAnnette Haardt-Becker et Simone Schulte, « Care and Treatment of Child Victims of Child Pornographic Exploitation (CPE) in Germany », Journal of Sexual Aggression, vol. 16, n° 2, juillet 2010, pp. 211–222.
- 91 Palmer, T., « Sexual Abuse and Exploitation in the Converged Online/Offline Environments: Referral services and rehabilitation », 2010 (document non publié, Centre de recherche Innocenti de l'UNICEF).
- 92 Quayle, E, L. Loof et T. Palmer, « Child pornography and exploitation of children online. A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents ». ECPAT International, Bangkok, 2008.
- 93 Microsoft Corporation, *Microsoft 2010 Corporate Citizenship Report*, Microsoft Corporation, Redmond VA (USA), 2010, p. 47; Cornell University Law School, Legal Information Institute, *Use to combat child pornography of technical elements relating to images reported to the CyberTipline*, U.S. Code, Titre 18, 1ère Partie, Chapitre 110, N° 2258C, disponible sur: <www.law.cornell.edu/uscode/usc\_sec\_18\_00002258---C000-.html>.
- 94 Maalla, N. M., « Report of the Special Rapporteur on the sale of children, child prostitution and child pornography », A/HRC/12/23, Nations Unies, New York, 13 juillet 2009, p. 12; disponible sur: <www.unhcr.org/refworld/docid/4ab0d35a2.html>, 1er septembre 2011.
- 95 Nissenbaum, H., « The Meaning of Anonymity in an Information Age », The Information Society, vol. 15, 1999, pp. 141–144, disponible sur: <www.nyu. edu/projects/nissenbaum/paper\_anonimity.html>, consulté le 22 septembre 2011.
- 96 Farfinski, S., UK Cybercrime Report, Garlik, Richmond, Royaume-Uni, n.d., disponible sur: <www.garlik.com/press/Garlik\_UK\_Cybercrime\_ Report.pdf>.
- 97 Voir par exemple: Police Commissioners'
  Conference Electronic Crime Working Party, « The
  Virtual Horizon: Meeting the law enforcement
  challenges Developing an Australasian law
  enforcement strategy for dealing with electronic
  crime », ACPR-RS-134.1, Australasian Centre for
  Policing Research, Payneham, Australie, 2000.
- 98 Entretiens avec le Centre de protection contre l'exploitation des enfants en ligne, mars 2011.

- 99 J. Von Weiler, A. Haardt-Becker et S. Schulte, « Care and Treatment of Child Victims of Child Pornographic Exploitation (CPE) in Germany », Journal of Sexual Aggression, vol. 16, n° 2, juillet 2010, pp. 211–222. Berggrav, S., Omsorg på nettet: Er det mitt ansvar?, Barnevernets utfordringer i å møte overgrepp på internett, Redd Barna (Care on the Internet: Is it my responsibility? The challenges of the Child Welfare Services in meeting online abuse, Save the Children Norvège), Oslo, 2010.
- 100 Palmer, T., « Sexual Abuse and Exploitation in the Converged Online/Offline Environments » (document non publié, Centre de recherche Innocenti de l'UNICEF).
- 101 Étude menée en septembre 2010 par Tink Palmer, Royaume-Uni, spécifiquement dans le cadre du présent document.
- 102 SaferNet Brasil, « Nética: Ethics and education for developing cyber-citizenship in Brazil », 2010, <a href="http://files.eun.org/insafe/blog/Netica.doc">http://files.eun.org/insafe/blog/Netica.doc</a>, consulté le 31 août 2011.
- 103 Child Protection Partnership (CPP) Digital Literacy Initiative, in collaboration with IICRDTrend Microsystems and Certiport Implementation by The Aspire Group Company (TAGC), 2010 (document non publié).
- 104 Odhiambo, Victoria, « Youth Mobilization to Promote Codes of Conduct in Internet Cafes in Africa », Presentation for Corporate Engagement in IT Companies Seminar, troisième Contrès mondial, ECPAT, Rio de Janeiro, 27 novembre 2008; disponible sur : <www.ecpat.net/WorldCongressIII/PDF/Publications/T4\_WS3c.pdf>, consulté le 31 août 2011.
- 105 Sharif, S., Cyber-Bullying, p. 256.
- 106 International Centre for Missing and Exploited Children, « Child Pornography: Model legislation & global review ».
- 107 Human Rights Council, « Joint Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, and the Special Representative of the Secretary General on Violence against Children », A/HRC/16/56, Nations Unies, New York, 7 mars 2011, disponible sur: <a href="http://srsg.violenceagainstchildren.org/document/a-hrc-16-56\_204">http://srsg.violenceagainstchildren.org/document/a-hrc-16-56\_204</a>>.
- 108 International Centre for Missing and Exploited Children, « Child Pornography: Model legislation & global review ».
- 109 Organisation internationale de police criminelle, « Notices & Diffusions », INTERPOL, Lyon, France, 22 juin 2011, disponible sur :

- <www.interpol.int/Public/Notices/default.asp>, consulté le 2 septembre 2011.
- 110 Conseil économique et social des Nations Unies, « Lignes directrices en matière de justice dans les affaires impliquant les enfants victimes et témoins d'actes criminels », Résolution 2005/20, Nations Unies, New York, 22 juillet 2005.
- 111 Rares sont les codes de bonnes pratiques mis au point au Royaume-Uni sous les auspices du Home Office Task Force sur la sécurité en ligne des enfants qui incluent des dispositions de surveillance. Cette approche a été expressément rejetée dans une étude menée en 2008 par le professeur Tanya Byron, disponible sur : <www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews>, et approuvée par la suite par le Bailey Review, <www.education.gov.uk/inthenews/inthenews/a0077662/bailey-review-of-the-commercialisation-and-sexualisation-of-childhood-final-report-published>.
- 112 Internet Watch Foundation, 2009 Annual and Charity Report, IWF, Cambridge, Royaume-Uni, 2009, disponible sur: <www.iwf.org.uk/assets/media/annual-reports/IWF%202009%20Annual%20 and%20Charity%20Report.pdf>.
- 113 Moore, T. et R. Clayton, « The Impact of Incentives on Notice and Take-Down », In Managing Information Risk and the Economics of Security, Springer, New York, 2009, pp. 199–223.
- 114 Voir par exemple: Using blocking to combat online child abuse images: Questions & Answers, Q3. Can't sites known to contain child abuse images just be taken down, as they are illegal?, ONG Européenne Alliance for Child Safety Online.
- 115 Moore, T. et R, Clayton, « The Impact of Incentives on Notice and Take-Down ».
- 116 Ofcom's Submission to Safer Children in A Digital World. p. 95.
- 117 Nyman, Anders, Abused Online, BUP Elefanten (Child and Adolescent Psychiatric Unit) et le County Council of Östergötland, n.d.; Palmer T., « Sexual abuse and exploitation in the converged online/ offline environments » (document non publié du Centre de recherche Innocenti de l'UNICEF).
- 118 Palmer T., « Sexual abuse and exploitation in the converged online/offline environments » (document non publié du Centre de recherche Innocenti de l'UNICEF).
- 119 Voir par exemple: Bureau de l'ombudsman fédéral des victimes d'actes criminels [Canada], Chaque image, chaque enfant, p. 30.
- 120 Lansdown, G., Article 12: The Right of the Child to be Heard: A resource book for governments, UNICEF/ Save the Children/HCDH, Londres, à paraître.



### **ACRONYMES**

CEOP Child Exploitation and Online Protection Centre – Royaume-Uni (Centre de protection

contre l'exploitation des enfants en ligne)

CRI Centre de recherche Innocenti (UNICEF)

ECPAT End Child Prostitution, Child Pornography and Trafficking of children for

Sexual Purposes

FSI Fournisseur de services Internet

INTERPOL Organisation internationale de Police criminelle

IWF Internet Watch Foundation

LGBT Lesbiennes, gay, bisexuels et transgenres

OPSC Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente

d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants

SRS Sites de réseautage social

TIC Technologies de l'information et de la communication

UE Union européenne

UIT Union internationale des télécommunications

### **GLOSSAIRE**

## Termes relatifs à l'abus et l'exploitation sexuels des enfants

Abuseur sexuel – Toute personne se rendant coupable d'actes répréhensibles de nature sexuelle contre des enfants ou ayant une activité sexuelle avec un enfant, communément appelé « pédophile » ; toutefois, comme il est précisé cidessus, les termes « auteur d'abus sur des enfants » ou « abuseur sexuel » sont plus appropriés. Il n'existe aucune définition de ce terme faisant l'objet d'un accord international.

Abus sexuel d'enfants en ligne - Production, distribution, téléchargement ou visionnement de matériel abusif d'enfants (images fixes ou vidéo), également appelé pornographie mettant en scène des enfants ; sollicitation en ligne d'enfants et de jeunes pour créer du matériel abusif d'enfants autoproduit, invitations à participer à des discussions sexuelles ou à d'autres activités sexuelles en ligne adressées à des enfants ou organisation de rencontres hors ligne à des fins sexuelles également appelées manipulation (grooming) ou leurre (luring), ainsi que la facilitation de l'un des actes décrits cidessus. Il n'existe pas de définition de l'abus sexuel d'enfants en ligne dans le droit international ; dans le présent rapport, le terme est considéré comme ayant l'acception ci-dessus.

Abus sexuel sur un enfant – Selon la définition de l'article 18 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201, ou « Convention de Lanzarote ») :

a) le fait de se livrer à des activités sexuelles avec un enfant qui, conformément aux dispositions pertinentes du droit national, n'a pas atteint l'âge légal pour entretenir des activités sexuelles;

(b) le fait de se livrer à des activités sexuelles avec un enfant :

- en faisant usage de la contrainte, de la force ou de menaces; ou
- en abusant d'une position reconnue de confiance, d'autorité ou d'influence sur l'enfant, y compris au sein de la famille; ou
- en abusant d'une situation de particulière vulnérabilité de l'enfant, notamment en raison d'un handicap physique ou mental ou d'une situation de dépendance.

Les dispositions du paragraphe (a) n'ont pas pour objet de régir les activités sexuelles consenties entre mineurs (article 18.3).

**Enfant** – Tout être humain âgé de moins de 18 ans, sauf si la majorité est atteinte plus tôt, en vertu de la

législation qui lui est applicable (article 1, Convention internationale des droits de l'enfant).

Environnement en ligne/hors ligne – Interface entre la communication passant par l'ordinateur et la communication directe (face à face). Si « en ligne » implique une communication non-physique, « hors ligne » sous-entend à l'inverse une interaction physique.

**Exploitation sexuelle des enfants** – La prostitution d'enfants, la pornographie mettant en scène des enfants et la participation d'un enfant à des spectacles sexuels, y compris le fait de recruter, de contraindre ou de faire participer un enfant à des spectacles pornographiques, d'en tirer profit ou d'exploiter un enfant de toute autre manière à de telles fins et le fait d'assister, en connaissance de cause, à des spectacles pornographiques impliquant la participation d'enfants ; le fait intentionnel de faire assister, à des fins sexuelles, un enfant n'ayant pas atteint l'âge légal pour entretenir des activités sexuelles, même sans qu'il y participe, à des abus sexuels ou à des activités sexuelles ; et la sollicitation d'enfants à des fins sexuelles (Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, articles 18-23).

Image abusive d'enfants – Représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles (voir « Pornographie mettant en scène des enfants » cidessous). Bien qu'il n'existe aucune définition faisant l'objet d'une convention internationale des termes « image abusive d'enfants », ce rapport les utilise de préférence à ceux de « pornographie mettant en scène des enfants » parce qu'ils ne laissent aucun doute quant au fait qu'un abus et une exploitation sont commis.

Manipulation en ligne – Formule définie par plusieurs auteurs et utilisée dans le présent rapport pour décrire un procédé destiné à inciter les enfants à adopter un comportement ou à participer à des conversations d'ordre sexuel à leur insu ou en toute connaissance de cause ou un procédé impliquant la communication et la socialisation entre le délinquant et l'enfant afin de rendre ce dernier plus vulnérable à l'abus sexuel. Le terme « manipulation » (grooming) n'est pas défini par le droit international ; certains États, dont le Canada, utilisent le terme « leurre » (luring).

**Pédophile** – Catégorie diagnostique désignant l'attirance ou préférence sexuelle d'un adulte envers les enfants pré-pubères. Le terme ne décrit pas avec précision les personnes qui abusent d'enfants via Internet et les technologies mobiles, et dont la

plupart sont mariés ou entretiennent des relations sexuelles à long terme avec des adultes. Par conséquent, dans ce rapport, les termes « auteur d'abus sur des enfants » ou « abuseur sexuel »

Pornographie mettant en scène des enfants -

Toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles (article 2, Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants). Dans le présent rapport, les termes « pornographie mettant en scène des enfants » ne sont utilisés que dans des citations ou lorsqu'il est fait référence à une législation spécifique, à un jugement ou à tout autre document qui utilise cette expression. En règle générale, l'expression « image abusive d'enfants » est privilégiée.

Prostitution des enfants – Le fait d'utiliser un enfant aux fins d'activités sexuelles contre rémunération ou toute autre forme d'avantage (article 2, Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants).

Sollicitation d'enfants à des fins sexuelles - Le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant n'ayant pas atteint l'âge légal pour entretenir des activités sexuelles, dans le but de se livrer avec lui à des activités sexuelles ou à la production de matériel de pornographie enfantine (Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, article 23).

Vente d'enfants – Tout acte ou toute transaction en vertu desquels un enfant est remis par toute personne ou tout groupe de personnes à une autre personne ou un autre groupe contre rémunération ou tout autre avantage (Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, article 2(a)).

#### Termes relatifs à l'environnement en ligne

Blog (blogue ou cybercarnet) - Site Web composé de notes ou de « billets », de textes et d'images, généralement affichés dans l'ordre chronologique. Des blogs entiers ou des notes spécifiques peuvent être publics et disponibles à toute personne en ligne, ou privés et accessibles uniquement aux utilisateurs autorisés par le propriétaire/auteur du blog.

**Cyberespace** – Univers virtuel partagé des réseaux informatiques mondiaux. Le terme « cyberspace » a été créé en 1984 par William Gibson, dans son roman Neuromancer. Le terme est souvent utilisé de façon interchangeable avec « Internet ».

E-mail - Contraction de « electronic mail » (ou courriel, contraction de courrier électronique), outil permettant d'envoyer un message ou e-mail à la boîte aux lettres électronique d'une autre personne par le biais d'un réseau de communication comme Internet.

En ligne – Contrôlé par ou connecté à un réseau informatique ou à Internet, et toute activité ou service disponible ou réalisé par le biais d'Internet. Une personne est « en ligne » dès qu'elle est connectée à un réseau d'ordinateurs ou a connecté un ordinateur ou un autre dispositif à Internet. Le terme hors ligne décrit toute activité non exécutée en ligne ainsi que le fait d'être déconnecté d'Internet.

Filtre - Mécanisme permettant de trier et de bloquer l'accès à certains contenus. La plupart des progiciels de contrôle parental utilisent une composante de filtrage ; le programme peut être conçu pour agir sur un ordinateur personnel individuel ou être appliqué à un réseau d'ordinateurs. Souvent, la composante de filtrage est fournie gratuitement comme partie intégrante du système d'exploitation de l'ordinateur ou est livrée avec le logiciel de connectivité proposé par le fournisseur de services Internet. Des filtres adaptés ont également été mis au point pour les téléphones portables et les consoles de jeux.

Forum de discussion interactif - « Salle de réunion » virtuelle dans laquelle il est possible de communiquer en s'envoyant des messages ou de discuter en temps réel. La plupart des forums de discussion interactifs abordent des sujets spécifiques mais certains sont plus généraux et sont créés pour fournir un forum de rencontre. Également appelé « salon de discussion ».

Fournisseur de services Internet (FSI) - Entreprise commerciale qui fournit aux utilisateurs un accès direct à Internet, en général contre rétribution, ou société qui fournit des services Internet comme l'hébergement ou le développement de sites Web.

Internet - Réseau mondial se composant de centaines de milliers de réseaux informatiques interconnectés utilisant une série de protocoles de communication communs et partageant un plan commun d'adressage. Internet facilite la transmission des courriers électroniques, des fichiers textes, des images et de nombreux autres types d'informations entre ordinateurs.

Large bande ou haut débit - Connexion numérique à haut débit qui facilite l'accès rapide à Internet et permet un échange plus rapide de fichiers volumineux, comme des vidéos, des jeux et des applications logicielles.

Médias sociaux - Outils développés principalement pour Internet et la mobilophonie afin de partager des informations et d'en discuter. Les termes « médias sociaux » se réfèrent le plus souvent à des activités comme la technologie, les télécommunications et l'interaction sociale et ils sont utilisés pour partager des textes, des images, des vidéos et des fichiers audio.

Messagerie instantanée – Service de communication utilisant le texte, similaire au forum de discussion

interactif. La principale différence est le fait que ces derniers sont généralement des espaces publics auxquels tout le monde peut participer tandis que la messagerie instantanée repose sur une « liste d'amis » ou une liste de personnes prédéfinie par l'utilisateur. Seules les personnes figurant sur cette liste peuvent communiquer avec l'utilisateur ; celui-ci choisit donc ses interlocuteurs et interlocutrices. Google Chat, MSN et Twitter sont des exemples de services de messagerie instantanée ; la plupart des sites de réseautage social (voir définition ci-dessous) possèdent une fonction de messagerie instantanée.

Messages textes – Messages de textes courts envoyés à l'aide de téléphones portables et d'appareils mobiles (comme SideKick) et les assistants numériques personnels (ordinateurs portables de base ou PDA).

Mondes virtuels – Environnement tridimensionnel simulé en ligne, habité par des joueurs qui interagissent entre eux par le biais d'avatars (icônes mobiles représentant une personne dans le cyberespace). Citons comme exemples Second Life ou Teen Second Life, plus populaire parmi les jeunes.

Navigateur – Logiciel sélectionné par le consommateur et utilisé pour localiser et afficher des pages du World Wide Web (pages Internet). Les navigateurs les plus populaires sont Windows Internet Explorer de Microsoft, Firefox, Google Chrome, Safari et Opera.

Partage de photos – Application qui permet aux utilisateurs de télécharger, de visionner et de partager des photos ; les utilisateurs peuvent octroyer un accès public ou privé.

Partage de vidéos – Application semblable au partage de photos (voir ci-dessus) mais pour les vidéos. Ces dernières sont souvent générées par l'utilisateur ; le plus grand site Web de partage de vidéos est YouTube.

**Pénétration** – Mesure dans laquelle une technologie est adoptée par les personnes pour lesquelles cette technologie est disponible.

Poste-à-poste (P2P) – Logiciel qui permet la transmission de données directement d'un ordinateur à un autre via Internet, généralement sans qu'il soit nécessaire de passer par un serveur tiers.

**Sexting** – Forme de messages textes (*voir définition ci-dessus*) par lesquels il est possible d'envoyer des images de nature sexuelle ou des textes sexuels explicites. Le sexting est une coutume particulièrement répandue parmi les adolescents. Également appelé « sexto ».

Short message service (SMS) – Service de messages textes courants disponibles sur les téléphones portables, autres appareils et ordinateurs portables.

Site de réseautage social (SRS) ou réseau social – Utilitaire en ligne qui permet à ses utilisateurs de créer des profils publics ou privés et de se constituer un réseau d'amis. Les réseaux sociaux permettent à leurs utilisateurs d'interagir avec leurs amis par des moyens publics ou privés, comme les messages et la messagerie instantanée, ainsi que de publier des contenus générés par l'utilisateur, comme des photos et des vidéos. Citons en exemple Facebook, MXit, Myspace et Orkut.

Smartphones – Téléphones portables dotés d'un système d'exploitation complet et capables d'accéder à Internet. Sous de nombreux aspects, ils ressemblent à de petits ordinateurs et possèdent des mémoires et des écrans plus grands que les téléphones ordinaires.

Technologies de l'information et de la communication (TIC) – Tout dispositif ou application de communication, incluant la radio, la télévision, les téléphones portables, les systèmes par satellite, ainsi que le matériel et les logiciels informatiques et de réseaux, de même que les services et applications connexes, comme la vidéoconférence et l'enseignement à distance.

Téléchargement (descendant) – Processus par lequel des données sont copiées sur un ordinateur en provenance d'Internet ou d'une autre source comme un lecteur externe, un disque, un téléphone ou d'autres appareils. Les données généralement téléchargées sur un ordinateur pour y être visionnées, stockées et accédées ultérieurement se composent de textes, de photographies, de vidéo et de musique.

**Téléchargement (montant) ou téléversement** – Processus de transmission des données à partir de l'ordinateur de l'utilisateur vers un serveur.

**Webcam** – Caméra vidéo intégrée ou connectée à un ordinateur, lui-même connecté à Internet.

World Wide Web (WWW) – Système basé sur l'hypertexte, qui permet de trouver et d'accéder à des données sur Internet. Le Web (ou la toile) héberge des documents, appelés pages Web, qui peuvent être reliés à d'autres documents ou systèmes d'information. Le Web n'est qu'une portion d'Internet et tous les serveurs d'Internet ne font pas partie du Web.

Centre de recherche Innocenti de l'UNICEF 12 Piazza SS. Annunziata 50122 Florence, Italie Tél. : (+39) 055 20 330

Fax: (+39) 055 2033 220 florence@unicef.org www.unicef-irc.org

ISBN: 978-88-6522-005-4

© Fonds des Nations Unies pour l'enfance (UNICEF) Mars 2012