

# Les enfants et l'Internet

*Internet occupe de plus en plus de place dans la culture d'aujourd'hui, surtout dans celle des enfants et des jeunes, pour qui les devoirs, les jeux en ligne et les réseaux sociaux comptent parmi les activités les plus populaires. Cependant, le manque d'accord commun relatif à la bonne façon d'aborder l'éducation et la protection des mineurs lorsqu'ils s'expriment ou sont actifs en ligne constitue un problème complexe. De plus, les différences culturelles et géographiques présentes dans les lois sociales reflètent le fait qu'il n'existe aucun point de vue universellement accepté de ce qui définit un enfant ou de ce qui est approprié pour un enfant. Ainsi, il est difficile de définir « des contenus et comportements inappropriés ».*

*Alors que certains délits sont naturellement considérés comme tels dans de nombreux pays et attirent donc une attention mondiale, les approches politiques au niveau national, qui visent à réguler les contenus n'ont fait, jusqu'à aujourd'hui, qu'exploiter une série de techniques de filtrage limitant ou bloquant l'accès à un contenu Internet. En outre, bien que l'on recommande au niveau local un filtrage institutionnel ou parental des outils informatiques (préférable au filtrage réseau), aucun de ces efforts ou méthodes de filtrage au niveau national et local n'est efficace à 100 % dans la régulation des contenus indésirables, car ils tendent parfois à sous- ou surbloquer les contenus. Le filtrage réseau provoque également des effets négatifs supplémentaires. Il est donc impératif pour les parents, les éducateurs, les tuteurs, les pairs et l'état d'informer les enfants et les jeunes des dangers et des responsabilités liées à l'utilisation d'Internet. Cette approche pourrait permettre aux jeunes de reconnaître et d'éviter les dangers et leur fournir les compétences informatiques nécessaires à une exploitation responsable des avantages offerts par l'activité sur Internet.*

## Introduction

L'Internet est un outil de communication très important pour les adultes comme pour les enfants. Aujourd'hui, les enfants et les jeunes utilisent fréquemment Internet pour :

- Apprendre (via l'accès à des informations, à des connaissances, des opinions, des outils éducatifs, voire même à une interaction avec des enseignants) ;
- Communiquer (exprimer des idées, partager des informations et des expériences) ;
- Interagir socialement avec des amis ou des pairs ;
- Innover, créer et partager des contenus ;
- Jouer et s'amuser (jeux, films, musique, livres, etc.).

Ces activités ont lieu de plus en plus souvent à l'extérieur de la maison ou de l'école, loin de l'ordinateur familial, sur des petits appareils mobiles, comme les smartphones et les tablettes.

Comparé à d'autres technologies d'information, comme la radio et la télévision, l'Internet offre aux parents, aux tuteurs et aux éducateurs des opportunités uniques de jouer un rôle plus direct dans la prise de décision de ce que leurs enfants peuvent voir et faire. Par exemple, ils peuvent diriger l'enfant vers des contenus intéressants et amusants, adaptés à son âge, sa culture, ses aptitudes

intellectuelles, son éducation, etc. L'Internet offre également la possibilité d'apprendre aux enfants à l'utiliser de manière constructive et les guide, afin d'éviter d'adopter des comportements risqués en ligne et d'accéder à des contenus inappropriés.

Il est d'une importance primordiale que tout le monde – parents, tuteurs, enseignants, institutions et gouvernements - travaille ensemble à la création d'environnements sûrs et accessibles aux enfants et aux jeunes où qu'ils se trouvent : chez eux, à l'école ou dans des établissements publics, tels qu'une bibliothèque ou un cybercafé. Il est de la responsabilité de tout un chacun de créer ces environnements pour que tous les enfants et les jeunes puissent profiter des aspects positifs de l'Internet et les exploiter.

De plus, bien qu'il soit important d'être vigilant quant aux risques potentiels encourus par les enfants qui utilisent Internet, il est tout aussi important de conserver une certaine perspective des choses. L'éducation, le bon sens et des directives claires sont les meilleurs outils de base. Bien que de nombreux efforts visant à protéger au mieux les mineurs aient été fournis, l'Internet Society estime qu'il est possible de mieux équiper les enfants et les jeunes afin qu'ils puissent à la fois se protéger des contenus potentiellement dangereux présents sur l'Internet tout en exploitant au maximum ses potentialités et qu'ils tirent le meilleur profit de sa valeur.

#### **Qu'est-ce qu'un « enfant » ?**

L'un des problèmes majeurs à affronter est celui de déterminer et de définir un « enfant » : en effet, les approches varient de manière significative selon les définitions sociétales et disciplinaires.

La Convention des Nations Unies sur les Droits de l'enfance (CDE) stipule à l'article 1 : « un enfant est un être humain de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt, en vertu de la législation qui lui est applicable ». Malgré les intentions bénignes de cette définition, fixer la limite d'âge à 18 ans est discutable selon de nombreux points de vue.

Naturellement, il existe d'autres définitions de l'enfant, mais chacune d'entre elles définit ce terme depuis une perspective scientifique différente. La psychologie, par exemple, adopte certains critères liés à la maturité et au développement psychologique, alors que la biologie montre une préférence pour le développement physique. D'un point de vue non-scientifique, les moralistes mettent en avant des notions de conscience et de liberté de consentement dans la détermination de ce qu'est un enfant.

#### **Utilisation de l'Internet par les enfants**

Il semblerait qu'un consentement sur ce qui définit une personne en tant qu'enfant représente l'un des plus grands obstacles à une protection infantile efficace. Peu importe la manière dont se définit le terme, nous savons avec certitude que les enfants et les jeunes utilisent régulièrement l'Internet, devenu une composante essentielle de la vie moderne. La capacité des enfants à accéder à Internet s'est rapidement accrue et la plupart des jeunes surfent fréquemment sur la toile.

Les enfants sont impliqués dans une vaste gamme d'activités sur Internet, dont la plupart se combinent entre elles. Les plateformes du Web 2.0 font de plus en plus partie de la culture jeune d'aujourd'hui. Un sondage effectué dans 25 pays et réalisé par *European Union Kids Online* et fondé par le « Programme pour un Internet plus sûr » de la Commission Européenne nous informe que les activités principales des enfants et des jeunes sur Internet sont les suivantes : devoirs (92 %), jeux en ligne (83 %), visionnage de vidéos (75 %) et réseaux sociaux (71 %).

59 % des enfants européens utilisant l'Internet possèdent leur propre profil sur un réseau social. 28 % seulement des 9-10 ans, mais 59 % des 11-12 ans ont un profil sur un réseau social, ce qui impliquerait que le moment où se déclenche l'envie d'interagir sur les réseaux sociaux se situe plutôt au début des études secondaires, plutôt qu'à l'âge fixé par la plupart des fournisseurs populaires<sup>1</sup>. Ainsi, l'identification et la mise en place de normes offrant des informations sur les interactions en ligne devraient faire partie intégrante de l'éducation d'un enfant et doivent commencer dès l'école primaire.

Afin d'assurer la sécurité des enfants sur l'Internet, l'une des approches les plus importantes est celle de les épauler dans la compréhension des concepts de risque et de sécurité en ligne, afin de les aider à prendre des décisions réfléchies et indépendantes. Une éducation en matière de sécurité sur Internet est fondamentale afin de protéger les mineurs contre les menaces en ligne, qu'il s'agisse de menaces extérieures, telles que des contenus ou activités « inappropriés » (par exemple, les jeux d'argent) ou de contacts avec les « mauvaises » personnes (p.ex. les intimidations, les traques, les arnaques) ou de menaces internes, telles que la divulgation excessive d'informations personnelles. En collaborant avec les enfants, en étant à l'écoute de leurs besoins et en se basant sur leur expérience, il est possible de modérer un environnement pour les mineurs et de leur permettre d'exploiter au maximum les opportunités offertes par l'Internet, en agissant de manière sûre et responsable. Parallèlement, un tel environnement peut être profitable aux enfants utilisant l'Internet pour commettre de « mauvaises actions » en les aidant à comprendre le véritable impact de leurs actes sur des personnes plus vulnérables.

Enfin, il est important de garder à l'esprit que l'Internet n'est pas un outil « diabolique », qui expose les enfants à des dangers sans précédent. Cette idée se base sur l'école de pensée basée sur la détermination et illustre comment « la préservation d'une capacité d'adaptation – à savoir la capacité de s'adapter à des changements de circonstances, tout en accomplissant ses objectifs principaux – [est] une aptitude essentielle à un âge rempli de bouleversements imprévisibles et d'inconstance »<sup>2</sup>. Selon cette théorie et en ce qui concerne la sécurité des enfants en ligne, légiférer et réglementer pourraient, à la fin, s'avérer être des pratiques contreproductives. Il est impossible (et potentiellement futile) d'essayer d'interdire toute activité pouvant éventuellement exposer les enfants au danger sur Internet. Une approche plus saine et plus durable se baserait au contraire sur des outils tels que l'éducation et l'autonomisation : ces pratiques permettraient aux parents, aux éducateurs ou à l'État d'affronter les problèmes liés à la sécurité des enfants sur Internet. Il faut tenter de mettre en place une familiarisation progressive des enfants à l'Internet et d'utiliser des stratégies de responsabilisation pour leur apprendre à affronter l'environnement numérique et ses dangers. À cette fin, apprendre aux enfants l'importance des « netiquettes » et leur inculquer la notion « réfléchir avant de cliquer » devrait être l'objectif principal.

Dans cette optique, les sections qui suivent illustrent quelques-uns des dangers encourus en ligne par les enfants.

### **Problèmes liés à la définition de la violence à l'égard des enfants et de la pornographie.**

La première tentative internationale visant à définir la « pornographie infantile » en tant que forme d'abus infantile a été celle du Protocole Facultatif (PF) à la Convention des Droits de l'Enfant (CDE)<sup>3</sup>, relatif à la vente d'enfants, à la prostitution et à la pornographie infantiles. Cependant,

<sup>1</sup> Statistiques complémentaires disponibles sur [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20 reports.aspx](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx)

<sup>2</sup> Andrew Zolli et Ann Marie Healy (2012). « *Resilience: Why Things Bounce Back* », Free Press,

<sup>3</sup> [http://www.unicef.org/crc/index\\_protocols.html](http://www.unicef.org/crc/index_protocols.html)

une définition plus récente émanant de la Convention du Conseil de l'Europe sur la Protection des enfants contre l'exploitation et les abus sexuels<sup>4</sup> a été ouverte à la signature en octobre 2007 et offre une plus grande clarté. L'article 20 définit la pornographie infantile comme « tout contenu représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ».

Ces pratiques étant généralement dissimulées et en l'absence d'une définition uniforme de ce qui doit être classé comme du contenu lié à des abus sexuels infantiles, il est difficile d'estimer l'étendue de la diffusion de ce contenu. À cette difficulté s'ajoute en outre le manque de données relatives à la production et à la distribution de contenus pornographiques infantiles dans de nombreux pays dans le monde, ainsi que la mutation globale constante en matière de production et de consommation de ces contenus. Le développement rapide des technologies de l'informatique et de la photographie numérique a ouvert la voie à la création aisée d'images générées ou modifiées numériquement, ce qui rend la collecte d'informations statistiques fiables sur l'ampleur du problème encore plus ardue.

De plus, le manque d'une législation nationale uniforme ou de contrôles au niveau mondial déclarant explicitement comme illégal le contenu pornographique infantile rend difficile la protection des mineurs sur l'Internet. Seules quelques nations ou régions ont introduit une législation criminalisant les contenus pornographiques infantiles. Bien que certains pays aient mis en place un processus de réforme légale, la plupart des États se basent encore sur une législation obsolète contre l'obscénité, en aucun cas adéquate à affronter les délits ou abus commis via l'Internet.

Le simple manque d'un accord clair au niveau gouvernemental en ce qui concerne l'ampleur du problème et d'une réponse légale appropriée ne fait qu'intensifier l'importance d'un suivi parental et éducatif des mineurs. Il est important de s'assurer que ces derniers sauront comment réagir s'ils doivent affronter en ligne un contenu pornographique infantile ou s'ils entrent en contact avec des personnes susceptibles de les impliquer dans des situations dangereuses.

### **Autres menaces potentielles**

Les enfants et les jeunes se trouvent face à un large éventail de risques lorsqu'ils utilisent un ordinateur. Ces risques sont parfois des menaces à l'encontre de leur sécurité ou de leur vie privée. D'autres peuvent provenir d'enfants violant intentionnellement ou involontairement les lois, telles que le droit d'auteur ou la diffamation. Ces risques peuvent également avoir de lourdes conséquences<sup>5</sup>.

#### *Quels sont les risques encourus par les enfants et par les jeunes ?*

- Une exposition à des images ou à un contenu inapproprié, que ce soit par inadvertance ou délibérément.
- Une sollicitation de la part de prédateurs sexuels via des salons de chat, via d'autres formes de médias sociaux ou par e-mail.
- Une intimidation ou un harcèlement en ligne.
- Le dévoilement inapproprié d'informations personnelles et le vol de données (par un partage trop important ou par d'autres moyens).

---

<sup>4</sup> <http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm>

<sup>5</sup> Des menaces de ce type sont significatives, mais dépassent les objectifs du document présent.

- Logiciels espions, virus et logiciels malveillants.
- Arnaques
- Mercantilisme excessif : publicités et sites Internet liés à des produits.
- Les conséquences de la tentation de se laisser impliquer par le piratage de logiciels, de musique ou de vidéos<sup>4</sup>.

La jeunesse est un groupe d'âge en pleine croissance qui utilise l'Internet. C'est lorsqu'il manque de conscience et dispose d'une aptitude limitée à évaluer le risque et à prendre des décisions que ce groupe est vulnérable. Une coopération entre divers intervenants au niveau local, national et international est une manière efficace de faire prendre conscience de l'importance des problèmes liés à la protection des mineurs dans certaines régions du monde. De plus, la répression des délits requiert une coopération policière en réseau au niveau local et national ; au niveau international, en revanche, une coopération et un partage d'informations est crucial en matière de protection des mineurs.

### **Il n'existe pas une seule approche relative à la protection des mineurs.**

Des différences culturelles et géographiques existent, liées à la fois au concept de l'enfance et à la perception de ce qui est considéré comme une pratique appropriée ou acceptable. Quant au contenu, et plus spécifiquement le « contenu inapproprié », une population de mineurs n'est pas homogène. Chaque enfant présente des différences – âge, éducation, langue, culture, religion, maturité, expérience, intérêts, etc. - et les individus changent rapidement en grandissant et en acquérant de la maturité. Les parents, tuteurs et éducateurs qui connaissent l'enfant sont les plus à même d'endosser la responsabilité de déterminer quel contenu lui est approprié.

La prolifération de nouvelles technologies, le décalage inévitable dans la mise en place de politiques les concernant et la diversité des cultures et des niveaux de développement soulignent la complexité de la recherche de solutions. D'un point de vue plus positif, il est également important de mettre en place et de publier des contenus culturellement et linguistiquement adaptés à l'âge des enfants, afin de les rendre attrayants et facilement accessibles.

### **Approches visant à contrôler l'accès à du contenu indésirable**

De nombreux pays dans le monde ont choisi de mettre en place des approches nationales de régulation de l'Internet avec des degrés variables de réussite et, parfois, avec des conséquences involontaires. On peut observer ce phénomène dans un nombre de pays toujours en augmentation qui ont choisi, ces dernières années, l'approche simpliste de limiter l'accès aux contenus en ligne. Ainsi, un nombre toujours croissant de pays a tenté d'imposer le filtrage sur Internet : une approche technique censée contrôler l'accès au contenu. Généralement, trois techniques sont communément utilisées pour bloquer l'accès à des sites Internet : le blocage de l'IP, le filtrage DNS et le blocage de l'URL par l'utilisation d'un proxy. Le blocage par mots-clés, qui bloque l'accès à des sites en se basant sur les mots trouvés dans les URL demandées ou qui bloque l'accès sur base d'une liste noire de termes, est une technique plus avancée utilisée par un nombre toujours plus important de pays. Ces méthodes peuvent être mises en place en différents endroits : par exemple, chez le FAI, par une institution, voire à l'emplacement où se trouve l'appareil spécifique connecté à Internet.

Il existe différentes techniques de filtrage et toutes visent à restreindre l'accès à certains sites Internet. Certaines techniques se basent sur une liste de « mauvais sites » créée par le FAI ou par les autorités et diffusée au niveau du réseau, mais les parents, tuteurs, éducateurs et autres autorités ont également accès à des programmes et à des outils visant à surveiller, traquer ou

bloquer l'accès à des activités en ligne spécifiques sur des appareils utilisés par des mineurs. Par exemple :

- Des proxys ou des logiciels pouvant autoriser ou bloquer l'accès à des sites ou protocoles spécifiques (tels qu'une protection antivirus, des filtres courriel antispam, des outils de blocage de fenêtres en incrustation, des logiciels anti-espion, des logiciels de suppression de cookies, etc.)
- Des logiciels de filtrage de contenu qui détectent et bloquent des contenus ou des sites spécifiques
- Des options de configuration permettant de configurer la confidentialité des sites et des critères de surveillance (p.ex., filtre Google SafeSearch, PrivoLock)

Cependant, le filtrage n'est jamais efficace à 100 %. Les technologies de filtrage sont sujettes à deux défauts inhérents : le sous-blocage et le surblocage. Le sous-blocage signifie que la technologie ne parvient pas à bloquer l'accès à tous les contenus ciblés. En revanche, les technologies de filtrage bloquent souvent du contenu qu'elles ne sont pas censées bloquer. Ce phénomène est appelé surblocage ou blocage excessif. Ces défauts surviennent parce que de nombreuses listes noires sont générées via une combinaison de sites Web désignés manuellement et via des recherches automatisées. Elles contiennent donc souvent des sites Internet y ayant été classés par erreur. Des problèmes supplémentaires surviennent lorsqu'un autre contenu est hébergé par la même adresse ou le même domaine IP. De plus, les méthodes de filtrage ne suppriment pas le contenu illégal de l'Internet<sup>6</sup>, et peuvent être contournées. Elles ont également le potentiel de restreindre involontairement ou délibérément les communications libres et ouvertes et par là même limiter les droits des individus ou des groupes minoritaires.

Les filtres réseau étant souvent brevetés et/ou utilisant des « listes noires » secrètes, il n'y a souvent aucune transparence en termes d'étiquetage et de restriction des sites Internet. Ce manque de transparence est particulièrement troublant lorsque les sociétés qui produisent ces technologies de filtrage de contenu travaillent en collaboration avec des régimes non démocratiques afin de mettre en place des schémas nationaux de filtrage de contenu. La plupart des états qui mettent en place le filtrage et le blocage de contenu agrémentent les listes de blocage générées commercialement avec des listes personnalisées se concentrant sur des sujets et des organisations spécifiques à un pays ou à une langue.

Bien que l'utilisation d'Internet à l'école soit généralement filtrée ou supervisée, de nombreux enfants ont accès à l'Internet depuis des emplacements différents et sur des appareils différents qui ne sont dotés d'aucun filtre et pour lesquels la supervision est limitée. Les enfants et les jeunes ont un accès de plus en plus important à Internet via d'autres appareils connectés, p.ex. des smartphones, des tablettes et des appareils de jeu vidéo. Cela signifie que même si le filtrage est actif sur l'ordinateur familial ou celui de l'école, les enfants et les jeunes ont tout de même la possibilité d'avoir accès à un Internet non filtré via d'autres dispositifs ou peut-être même sur ces mêmes ordinateurs en contournant les filtres mis en place. Il est donc primordial d'enseigner aux enfants le bon comportement à adopter en ligne et de les inciter à discuter des problèmes auxquels ils pourraient être confrontés.

Le filtrage réseau, tel que le filtrage DNS, cause également une instabilité du réseau, encourage la fragmentation et mine les fondations de l'Internet<sup>7</sup>. D'autres approches de contrôle du contenu,

<sup>6</sup> Un nom de domaine différent pointant vers la même adresse Internet peut être créé en quelques minutes.

<sup>7</sup> Pour plus d'informations sur le blocage DNS, consulter la page : <http://www.internetsociety.org/what-we-do/issues/dns/finding-solutions-illegal-line-activities>

telles que la saisie du nom de domaine, dont la conception ne vise pas uniquement à protéger les jeunes, souffrent pour la plupart des mêmes problèmes que le filtrage DNS : contournement aisé, incapacité à résoudre le problème sous-jacent et incitation à la création d'un réseau fantôme hors de portée de la loi.

Bien que les logiciels soient capables de bloquer des sites Internet spécifiques à forte visibilité, il n'existe actuellement aucune solution durable dans le temps ou totalement efficace. Ces technologies sont incapables d'identifier et de cibler précisément des catégories de contenu spécifiques trouvées sur les milliards de sites ou autres applications Internet, tels que les groupes d'information, les listes courriel, les salles de chat, les messageries instantanées et les médias sociaux. Le filtrage ne remplace jamais une bonne implication et les judicieux conseils parentaux. Dans tous les cas, ces méthodes ne suppriment pas les contenus répréhensibles ou illégaux d'Internet, elles ne font qu'en rendre l'accès moins aisé.

Enfin, l'Internet Society s'inquiète du fait que la protection des mineurs en ligne puisse devenir une porte d'entrée ou de sortie pour d'ultérieurs contrôles gouvernementaux en ligne. Cela dit, les enfants et les jeunes ne peuvent être protégés à 100 % par le blocage de contenu lorsqu'ils sont sur Internet. Nous pouvons pourtant améliorer la sécurité des mineurs sur Internet en donnant les moyens aux enfants, aux parents, aux tuteurs, aux éducateurs et aux pairs d'identifier et de gérer les contenus nuisibles sur les ordinateurs, l'Internet et les téléphones mobiles, en leur apprenant à utiliser la technologie de manière sûre et responsable et en mettant à leur disposition des outils de gestion de l'accès et du contenu adaptables et faciles d'utilisation.

### Politiques récentes

En 2011, l'OCDE a publié un rapport intitulé *La protection des enfants sur Internet : risques affrontés par les enfants sur Internet et politiques visant à les protéger*<sup>8</sup>. En 2012, l'OCDE a adopté une *Recommandation du Conseil sur la protection des enfants sur Internet*<sup>9</sup> et a établi trois principes clés :

- Autonomisation ;
- Proportionnalité et valeurs fondamentales ;
- Flexibilité.

De plus, cette Recommandation<sup>10</sup> fait appel aux gouvernements pour qu'ils :

- fassent usage de leurs qualités de dirigeants et témoignent d'un engagement à travers leurs politiques ;
- soutiennent une réponse coordonnée émanant de tous les intervenants ; encouragent l'uniformité et la cohérence des initiatives nationales de protection des mineurs sur Internet parmi les intervenants publics et privés ;
- encouragent la prise de conscience et l'éducation en tant qu'outils essentiels pour l'autonomisation des parents et des enfants ;
- soutiennent des politiques factuelles lors de la protection des enfants sur Internet ;
- encouragent le développement et l'adoption de technologies de protection des enfants sur Internet qui respectent les droits des mineurs et la liberté des autres utilisateurs d'Internet ;

<sup>8</sup> [http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online\\_5kgcjf71pl28-en](http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en)

<sup>9</sup> <http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>

<sup>10</sup> <http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>

- renforcent les réseaux internationaux des organisations nationales consacrées à la protection des enfants sur Internet ;
- partagent des informations concernant les politiques nationales de protection des enfants sur Internet, et, en particulier de développement des bases empiriques pour une analyse politique internationale comparative, quantitative et qualitative ;
- soutiennent les efforts de renforcement de compétences au niveau régional et international et les mesures opérationnelles prises en matière de protection des enfants sur Internet ;
- coordonnent mieux le travail effectué par les diverses organisations internationales et régionales et par les entités jouant un rôle dans le soutien des efforts gouvernementaux dans ce domaine et impliquent les intervenants non-gouvernementaux le cas échéant.

### **Autonomisation des enfants : un rôle constructif pour les parents, les tuteurs et les éducateurs**

La manière la plus efficace d'affronter les problèmes ressentis dérivant de l'utilisation d'Internet est d'autonomiser les enfants et les jeunes afin qu'ils sachent comment se protéger et protéger leurs amis. Les techniques d'autonomisation comprennent un enseignement des limites légales dans un langage approprié à l'âge de l'enfant, ainsi qu'une discussion ouverte sur les règles et attentes morales, culturelles et éthiques de leurs communautés. Le rôle des parents, des éducateurs, du secteur privé, des gouvernements et autres est celui d'aider les jeunes à apprendre à reconnaître et à respecter ces règles et limites. L'autonomisation des enfants et des jeunes leur permet également d'éviter de devenir des victimes d'autres menaces, telles que les arnaques, les logiciels espions ou malveillants.

Bien qu'il y ait une émergence de stratégies permettant aux parents de gérer l'utilisation d'Internet par leurs enfants, les tactiques de ces derniers pour contourner ou résister à cette supervision familiale se développent également. Ce problème se complique ultérieurement par le fait que les enfants connaissent souvent mieux ces nouveaux médias et les utilisent avec plus d'expertise que leurs parents. Toutefois, les enfants et les jeunes ont généralement des relations de confiance avec des adultes et des pairs dont ils estiment les conseils et opinions (personnes exerçant une influence de confiance). Il est important que les personnes qui exercent ces influences de confiance soient eux-mêmes conscients des risques et des solutions potentiels et aient été formés à la manière de transmettre les informations à ceux qui les considèrent comme un modèle et une source d'informations et de conseils fiables. Il est également important d'admettre que les personnes exerçant ces influences de confiance vont changer dans le temps. Plus un enfant approchera de l'adolescence, plus ses pairs exerceront une influence forte sur eux.

En outre, les parents, tuteurs, éducateurs et personnes exerçant une influence de confiance devraient participer activement à enseigner aux enfants et aux jeunes les risques qu'ils peuvent encourir en présence de matériel sexuellement explicite ou de prédateurs et arnaqueurs sur Internet et la manière dont ils peuvent les éviter. Il est tout aussi important d'enseigner aux enfants la manière de communiquer de manière privée avec des amis connus et de faire preuve de prudence lors du partage d'informations personnelles sur Internet. Bien entendu, pour un enseignement efficace, il est important que les parents, les tuteurs, les éducateurs et les pairs aient une bonne compréhension du fonctionnement des outils informatiques.

Deux facteurs au moins posent problème aux parents dans leur aptitude à contrôler l'accès et l'utilisation d'Internet de leurs enfants. Le premier est que, bien que les parents soient responsables de la sécurité de leurs enfants, ils doivent également respecter leur indépendance croissante et leur droit à une certaine confidentialité.



Le second est le fait que peu de parents comprennent entièrement la culture Internet de leurs enfants<sup>11</sup>. L'utilisation faite par les enfants et les jeunes des réseaux sociaux est souvent déroutante pour les parents. De plus, l'attitude adoptée vis-à-vis de la vie privée, de la confidentialité et des droits de l'individu sur les données possédées et partagées subit d'immenses écarts générationnels. Les problèmes de la sécurité, de la vie privée, de la prédation et de l'intimidation en ligne sont complexes, à la fois techniquement et psychologiquement, et les parents peuvent avoir beaucoup de mal à s'en sortir. Ces facteurs signalent un besoin urgent d'encourager les parents à engager la conversation avec leurs enfants et aborder le sujet de leurs activités en ligne, peu importe leur niveau d'expérience. Cette implication permettra aux parents, aux tuteurs, aux éducateurs et autres personnes exerçant une influence de confiance de maintenir les enfants et les jeunes loin du danger.

Parallèlement, il est important que les enfants aussi aient de bonnes connaissances en matière d'utilisation de l'outil informatique. Ces connaissances incluent un enseignement et un encouragement à maîtriser les outils de TIC disponibles et à prendre les bonnes décisions (seul(e) et en groupe), afin qu'à l'avenir, les enfants deviennent la nouvelle génération de personnes exerçant une influence responsable et de confiance.

### **Conclusion**

Bien qu'un travail direct soit mis en place avec les enfants au sein des familles, des écoles et d'autres environnements où sont prodigués des conseils et où une interaction en face à face est possible, il serait souhaitable que les gouvernements, les associations à but non-lucratif et les organisations communautaires entreprennent une série d'actions visant à favoriser la prise de conscience et le développement des compétences afin d'aider les enfants et les jeunes à utiliser Internet dans un environnement sûr. Ci-après sont mentionnés quelques exemples d'initiatives qui pourraient être envisagées :

- Impliquer tous les intervenants dans des activités de prise de conscience communautaire : agences gouvernementales, secteur Internet privé, ONG, groupes communautaires et le grand public<sup>12</sup>.
- Mettre en place des permanences téléphoniques ayant trait à l'Internet, afin de soutenir le public lors du signalement de délits sur Internet et de fournir conseils et assistance.
- Encourager les programmes éducatifs impliquant les FAI et la mise en place de lois visant à développer les meilleures pratiques dans la gestion de contenus et comportements illicites.
- Mettre en place des sites ou plateformes Internet afin d'offrir aux enfants, aux adolescents, aux parents et aux enseignants une base éducative. Le contenu de ces sites, relatif à la sécurité sur Internet, devrait être à jour et régulièrement actualisé avec des vidéos d'auto-apprentissage dans différentes langues régionales.

L'Internet change si rapidement qu'il est probable que les mesures technologiques ne parviennent pas à suivre le rythme. Les mesures les plus efficaces et les plus durables sont celles qui se construisent au sein de la famille, qui impliquent la communauté, l'éducation et l'autonomisation, afin que les enfants et les jeunes puissent faire les bons choix et profiter de la puissance génératrice de l'Internet.

---

<sup>11</sup> Les manières dont leurs enfants utilisent l'Internet et le téléphone mobile pour travailler, jouer et socialiser

<sup>12</sup> Pour des exemples de bonnes pratiques sécuritaires sur Internet, consulter le site [www.kidsap.org](http://www.kidsap.org) et le manuel ECPAT International's Safety Online Handbook.

## **Annexe**

### **« Signaux et Indices » pour les parents, les enfants et les éducateurs**

Vous trouverez ci-dessous quelques astuces relatives à l'utilisation d'Internet pouvant être utiles aux parents, aux enseignants (et aux enfants).

- Il est préférable que l'ordinateur se trouve dans un endroit visible de la maison, afin que les adultes puissent superviser l'utilisation qui en est faite.
- Il serait bon de fournir un enseignement de ce que sont les ordinateurs et de la manière dont Internet doit être utilisé à tous les niveaux – enfants, parents et enseignants.
- Les parents et enseignants devraient passer du temps avec leurs enfants dans l'environnement numérique.
- Il est du devoir des parents de fixer des limites de temps et d'utilisation d'Internet (en concertation avec leurs enfants).
- Les parents et éducateurs devraient apprendre à reconnaître et à se familiariser avec les dangers d'Internet.
- Les parents et éducateurs se doivent d'insister sur le fait que le principe « Ne pas parler aux étrangers » s'applique également à l'environnement numérique.
- Les parents et éducateurs doivent interdire à leurs enfants de télécharger et/ou de mettre en ligne des photos sans supervision préalable.
- Une utilisation intégrale des contrôles de filtrage et parentaux doit être mise en place à la fois à la maison et dans les milieux scolaires.
- Les parents et les éducateurs ont l'obligation d'instiller aux enfants le besoin d'intimité à un jeune âge, en leur expliquant pourquoi il est important qu'un enfant respecte et sollicite le droit d' « être seul(e) ».

Internet Society  
Galerie Jean-Malbuisson 15  
CH-1204 Genève, Suisse  
Tél. : +41 22 807 1444  
Fax : +41 22 807 1445  
<http://www.internetsociety.org>

1775 Wiehle Ave. Suite 201  
Reston, VA 20190, USA  
Tel : +1 703 439 2120  
Fax : +1 703 326 9881  
e-mail : [info@isoc.org](mailto:info@isoc.org)