Autorité Nationale pour
la Protection des Données
et la Liberté de l'Information

LA CLEF DU CYBERESPACE

Étude de la NAIH
pour un usage sûr et conscient d'Internet par les enfants

2013

La clef du cyberespace

Étude de la NAIH
pour un usage sûr et conscient d'Internet par les enfants

(Pour la promotion d'un usage d'Internet par les enfants conscient de leurs droits et devoirs par les moyens de la protection des droits fondamentaux)

2013

Objectif de l'étude :

Sensibiliser les enfants aux dangers potentiels d'Internet, identifier les enjeux du futur, promouvoir un usage conscient d'Internet et l'exercice par les citoyens de leurs droits, par la mise en œuvre des résultats de recherches théoriques et pratiques.

Contributions :

Viktor Árvay (NAIH)

Nóra Belső (psychiatre)

Laura Kozma (NAIH)

Ágnes Lux (Bureau du Commissaire aux droits fondamentaux)

Petra Márkus (NAIH)

Attila Mátyásfalvi (NAIH)

Borbála Csekeő Reményiné (Fondation Kék Vonal Child Crises)

Gabriella Sárközi (experte en médiation pédagogique)

Dániel Somfalvi (NAIH)

Katalin Somogyvári (NAIH)

Júlia Sziklay (NAIH)

Zsófia Tordai (NAIH)

Direction de l'étude:

Júlia Sziklay

Traduction:

Julien Rossi

Table des matières

Présentation de l'Autorité Nationale pour la Protection des Données et la Liberté de l'Information....1
Présentation du sujet d'étude....2
Présentation de quelques cas étudiés....3
Méthodologie....5
L'environnement en ligne des enfants....6
Les aspects positifs d'Internet....6
Les droits des enfants sur Internet....7
Panorama des principales questions de fond....9
A. Âge et maturité....9
B. La question de l'anonymat : est-ce plus facile avec un masque ?....9
C. Troubles de la personnalité....10
D. Espaces publics, amis inconnus....11
E. Les contenus nuisibles....12
F. Tendances prévisionnelles....12
Panorama des principales déviances sur Internet....14
A. Le harcèlement sur Internet....14
B. Le phénomène des mèmes....14
C. Les trolls....15
D. L'envoi d'images de nature sexuelle (sexting)....15
E. La pédophilie sur Internet....15
F. Infiltration et fausse identité (grooming)....16
G. Les jeux en ligne destinés aux enfants....16
H. Autre formes d'abus en relation avec la protection des données personnelles....17
Panorama des bonnes pratiques à l'international....18
A. Portugal. Projet « DADUS »....18
B. Irlande. Projet « Private I, Public Eye »....18
C. Écosse. Projet « Respect Me »....19
D. Norvège. Projet « You Decide »....19
E. Nouvelle-Zélande : « Youth Privacy Kit »....19
F. Canada : bandes dessinées et conseils....20
G. États-Unis d'Amérique....20
H. Union européenne....21
La recette hongroise....22
ANNEXES....24

Présentation de l'Autorité Nationale pour la Protection des Données et la Liberté de l'Information

L'Autorité Nationale pour la Protection des Données et la Liberté de l'Information, dont le nom est abrégé sous la forme de l'acronyme *NAIH*[1] en hongrois, a commencé à fonctionner le 1er janvier 2012. Elle prend la suite en matière de protection des droits fondamentaux à la protection des données et à la liberté de l'information du Commissaire à la protection des données, qui a existé entre 1995 et 2011. Suivant les dispositions de la Loi Fondamentale et de la loi de protection des données[2], elle est l'autorité d'État responsable de la supervision de la protection des données à caractère personnel (il s'agit du volet de protection des données de ses activités), de l'accès aux documents administratifs (liberté de l'information) et de la garantie de l'exercice de ces libertés fondamentales et constitutionnelles. Elle reçoit et examine les plaintes des citoyens. Dans le cas d'infractions graves aux règles sur la protection des données, elle a le pouvoir de lancer une procédure administrative pouvant aboutir à des sanctions comme l'arrêt d'un traitement illégal de données, l'effacement de ces données, l'interdiction de traiter des données personnelles voire des amendes dont le montant maximal est fixé par la loi à dix millions de forints, soit à peu près 33 000 euros (montant en vigueur en février 2014).

Au regard du nombre incroyablement élevé d'informations, de traitements de données et de personnes impliquées, mais aussi de la force sans limites du caractère public de ce qui s'y trouve, Internet est sans conteste le lieu par excellence du traitement des données personnelles et de l'information publique. Pour les acteurs de la protection des données à caractère personnel, la protection de celles des mineurs relève d'un niveau particulier de priorité. En effet, en raison de leur âge et du manque d'expérience qui en est la conséquence, ces personnes sont par définition les plus fragiles face aux conséquences d'infractions dont elles peuvent être victimes. Ces conséquences peuvent notamment porter sur leur développement personnel. Il nous paraît donc évident que les autorités de protection des données à caractère personnel doivent se saisir avec attention de la question du traitement des données des mineurs sur Internet. Le rôle de la prévention et de la diffusion d'informations est crucial. Trouver des remèdes aux infractions commises, et attirer l'attention des intéressés et de l'opinion publique sur ces sujets sont une de nos missions fondamentales.

1 Nemzeti Adatvédelmi és Információszabadság Hatóság

2 Loi CXII de 2011 portant autodétermination informationnelle et liberté de l'information
Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

Présentation du sujet d'étude

> « Internet n'est ni bien ni mal – il est simplement symptomatique. C'est un miroir. Il semble que l'usage qui en est fait n'est pas radicalement nouveau. L'existence sur la toile hérite de l'existence sociale ses fardeaux et ses misères. »
>
> – Dr. László ROPOLYI[3]

Ces dernières décennies, le développement rapide de l'informatique, d'Internet et des télécommunications a provoqué des changements radicaux dans le monde. Les symptômes fondamentaux de la société de l'information sont l'abondance et la diffusion pratiquement illimitées de l'information. « Ce n'est pas le rôle central de la connaissance et de l'information qui caractérise la révolution technique actuelle, mais l'utilisation de la connaissance et de l'information pour créer de nouvelles connaissances et de nouveaux outils d'information et de communication »[4], écrit Manuel Castells sur cette société de l'information dans laquelle nos enfants naissent aujourd'hui, et pour qui il s'agit d'un moyen de communication naturel.

Il est possible sans exagérer les résultats des études à notre disposition (comme l'étude « European Values Study » de 2008[5]) d'affirmer que l'individu communiquant et ayant une vie sociale sur Internet, si ce n'est que par la force de la quantité des informations auxquelles il se trouve confronté, est quelqu'un de plus curieux, plus ouvert sur les nouveautés. Mais il est parallèlement moins prudent que ses semblables n'utilisant pas Internet. Des études internationales se concentrant principalement sur les enfants[6] nous avertissent sur le risque d'existence auprès des internautes d'un phénomène de « dualité morale ». Les normes morales d'un usager fréquent d'Internet sont plus tolérantes, moins strictes, que les règles auxquelles la même personne s'astreint hors-ligne. Cela s'observe dans le téléchargement illégal systématique de logiciels, dans la grossièreté stylistique des textes tchattés, dans les commentaires injurieux, voire dans le harcèlement en-ligne, ou dans l'usage abusif des données personnelles des ses pairs sur le Net[7].

La nouvelle culture génère avec elle de nouveaux comportements. En tant qu'adultes, nous devons connaître et comprendre ces phénomènes, et être capables de préparer la nouvelle génération[8] à faire face à ses éventuels dangers. Heureusement, de nombreux programmes, campagnes d'information et organismes s'y intéressent, y compris en Hongrie.

---

3 ROPOLYI, László, « Internet-használat és hálólét-konstrukció », in : *Információs társadalom*, VI(4), 39-46, 2006

4 CASTELLS, Manuel : *A hálozati társadalom kialakulása*, Gondolat-Infonia, 2005, p. 68 (TDA)
Disponible en français : CASTELLS, Manuel, *L'ère de l'information, la société en réseaux*, Paris:Fayard, 2001, 671 pages

5 CSEPELI, György et PRAZSÁK Gergő, « Internetezők az értékek vonzásában » in ROSTA Gergely et TOMKA Miklós, *Mit értenek a magyarok ? Az Európai Értékrend Vizsgálat 2008. évi magyar eredményei*, Budapest:OCIPE Magyarország-Faludi Ferenc Akadémia, 2010, pp. 187-204

6 Par exemple : MICHELET, Isabelle, *Our Children at Risk Online : The Example of Thailand*, Bangkok:ECPAT International, 2003

7 « Il manque aux enfants qui passent beaucoup de temps sur Internet la faculté d'empathie et la possibilité de lire les visages. Ils ne peuvent pas ressentir les signaux subtils que les êtres humains transmettent de façon non-verbale et non-écrite. Ceci génère un grand nombre de conflits hors-ligne ». Citation de : PARTI, Katalin et VIRÁG, György, A szájbergyerek és a bicikli. A kelet-európai gyerekek nethasználatának specifikumai, *Kriminológia tanulmányok* n°48, Budapest:OKRI, 2011, p. 43

8 *La génération Y correspond à la nouvelle génération, née entre 1976 et 1995, sur laquelle le développement des nouvelles technologies a eu un impact fort, et la génération Z est la première génération globalisée, née dans la société de l'information entre 1995 et 2009, et qui sont aujourd'hui généralement à l'âge de l'adolescence.*

Le but de cette étude est de contribuer de façon pertinente à l'analyse contemporaine du sujet en adoptant le point de vue des droits fondamentaux, et plus particulièrement, du droit fondamental à la protection des données à caractère personnel. Au-delà de ces aspects théoriques, nous souhaitons contribuer à l'amélioration de la culture numérique des enfants par le développement d'outils pratiques. Avec l'appui du ministère en charge de l'éducation, nous envisageons ainsi d'organiser des présentations de cette étude en milieu scolaire. Notre approche part du respect de la dignité humaine, qui est un principe fondamental du droit hongrois, inaliénable et illimité. De ce droit découle le droit à la protection des données personnelles. Si les enfants qui utilisent Internet sont sensibilisés à ces valeurs, alors ils ne commettront pas d'actes pouvant blesser la dignité d'autrui. Il saura même se protéger de façon consciente des phénomènes d'agression qui l'entourent, ce qui diminuera significativement sa situation de faiblesse.

Présentation de quelques cas étudiés

La NAIH a examiné un grand nombre de cas, parvenus auprès des autorités de protection des données ou des autorités judiciaires, dans lesquels le droit d'enfants à la protection de leurs données personnelles avait été enfreint. Ce chapitre a pour objectif de présenter un échantillon des infractions sur Internet dont les mineurs peuvent être victimes.

Exemples de cas ayant été traités par l'autorité hongroise de protection des données

La NAIH, en tant qu'autorité indépendante de protection des données personnelles, reçoit et instruit les plaintes adressées par les citoyens dont les données personnelles ont fait l'objet d'une utilisation contraire à la loi. Pour l'essentiel, ces plaintes concernent des abus d'utilisation de données mises en ligne sur des réseaux sociaux. À ce sujet, la NAIH considère que le niveau de publicité des données publiées sur ces réseaux doit être interprété dans un sens restrictif : seuls les utilisateurs inscrits sur ces réseaux et auxquels le sujet des données personnelles a accordé l'accès, ou bien les personnes autorisées expressément par la loi, ont le droit d'y accéder. La diffusion à un cercle plus large de ces données ne peut se faire sans le consentement de l'individu concerné, sans enfreindre les règles de droit hongroises.

- Un parent ayant mis en ligne une photo de sa fille sur un réseau social, s'est plaint de sa publication par un tiers sur un site Internet public, accompagnée de commentaires injurieux. Le propriétaire du site Internet refusa de donner suite aux demandes de suppression adressée par ce parent. Il publia le texte de ces demandes adressées par courrier avec l'adresse d'expédition, accompagnés de propos injurieux et diffamatoires (ABI-7041/P/2010)
- Une plaignante s'est tournée vers le Commissaire à la protection des données après que des photos d'elle se soient retrouvées sur le site www.puruttya.hu à côté d'images pornographiques. Ces images correspondaient à celles qu'elle avait mises en ligne dans le cadre d'un concours de beauté sur le réseau social MyVip. Le responsable éditorial de ce site Internet ne donna pas suite aux demandes de suppression (ABI-4900/2010/P)
- La NAIH a prononcé en 2013 une sanction pécuniaire de 3 millions de forints contre Generál Média Publishing Kft. Un des motifs de la sanction était la présence de quelques

3500 profils d'enfants âgés entre 10 et 15 ans, en l'absence d'autorisation parentale, sur des sites de rencontres en ligne. La création d'un profil pour le compte de l'enquête a révélé dans les jours qui suivent l'arrivée de messages à caractère sexuel, certains relevant du harcèlement. La NAIH considère donc que parmi les réseaux sociaux, les sites de rencontres en ligne sont les plus susceptibles de présenter un danger pour des mineurs.

Exemples de cas traités par le Médiateur

L'institution d'un Médiateur remonte en Hongrie à 1995, dont le titre officiel depuis 2012 est celui de Commissaire aux droits fondamentaux. Il peut être saisi ou se saisir de tout dossier ou plainte relatif à la violation des droits fondamentaux, et émettre des avis en vue de permettre la résolution de ces problèmes. En l'absence d'institution spécifique, c'est le Médiateur qui est chargé de surveiller la bonne application du droit des enfants en Hongrie. Plusieurs cas examinés dans ce cadre nous ont intéressé. À titre d'exemple, en janvier 2011, un plaignant s'est tourné vers le Médiateur dans le cadre de courriers électroniques indésirables (*spams*) à caractère sexuel envoyés à son enfant mineur. L'état actuel du cadre légal et technique n'ont cependant pas permis de trouver de solution satisfaisante à la requête du plaignant.

Exemples de cas portés à la connaissance de la police

À notre demande, le Commissariat central de la police nationale (ORFK) nous a fait parvenir un aperçu des délits et crimes commis sur Internet ayant pour cible les mineurs. Il s'agit généralement d'infractions mineures participant à la réalisation d'un délit ou crime plus important.

La première étape est la collecte d'informations et donc de données personnelles sur ces enfants. Plusieurs techniques peuvent être employées à cet effet, comme la création de portails en ligne dédiés, par exemple contenant des jeux vidéos, l'usurpation d'identité, ou encore la diffusion de chevaux de Troie. Les données sont ensuite échangées sur un marché noir. L'ORFK nous a également rapporté des cas dans lesquels un pirate prenait le contrôle de la webcam de sa victime pour réaliser à son insu des vidéos compromettantes, pouvant alors servir de monnaie d'échange.

La seconde étape est constituée par l'exploitation des données collectées. Les exemples de crimes commis par ce biais vont de l'extorsion de fonds à l'usurpation d'identité en passant par le harcèlement sexuel, l'atteinte à la pudeur et la pédopornographie.

Conclusion

Ce bref aperçu des cas ayant fait l'objet d'une plainte en Hongrie montrent que les infractions dont peuvent être victimes les mineurs vont de la simple atteinte au droit à l'image à l'extorsion de fonds ou à des crimes sexuels. Dans l'ensemble de ces cas, une mauvaise utilisation d'Internet, par exemple une mauvaise sécurisation de ses données (mot de passe faible, mauvaise configuration de paramètres de confidentialité, navigation sur des sites non-vérifiés…), facilite le travail des criminels.

Méthodologie

La NAIH a publié en 2013 une étude de 121 pages sur le thème de la protection de l'enfance sur Internet. Dans un premier temps, nous avons voulu comprendre les aspects légaux des dangers menaçant les enfants sur Internet. Nous avons ensuite dressé une typologie de comportements déviants contre lesquels nous devons agir.

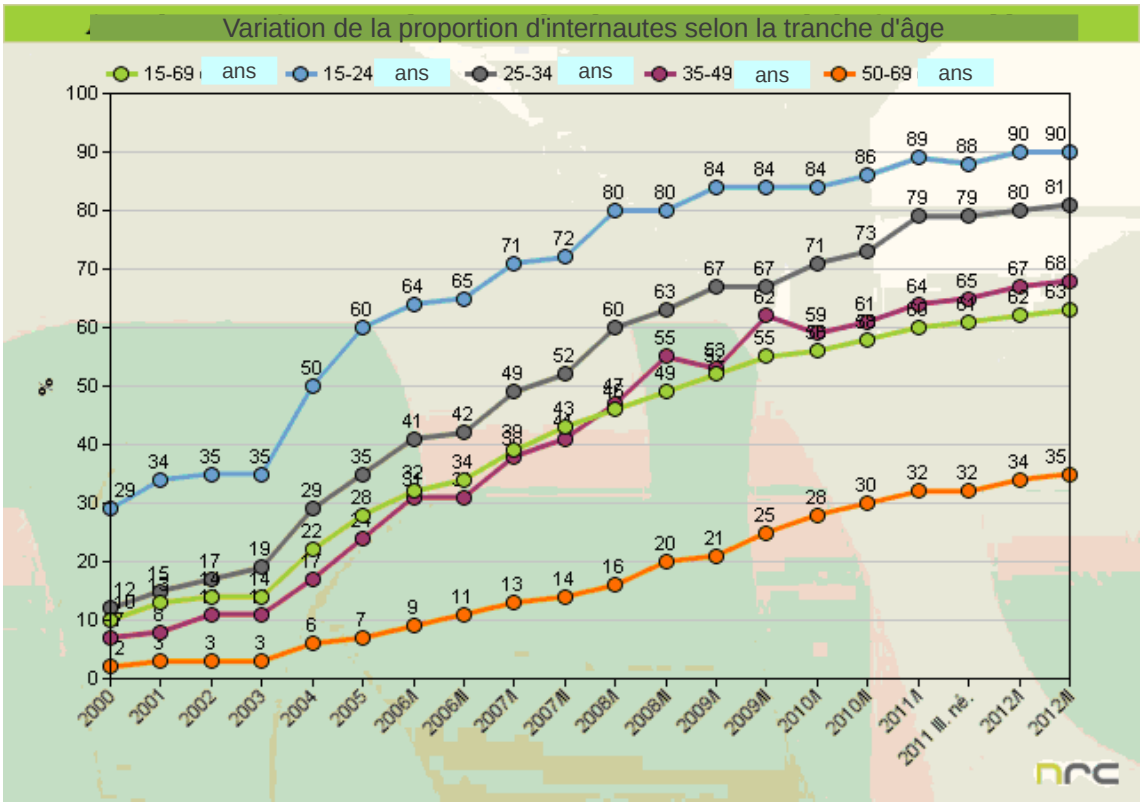
Une fois ce travail de reconnaissance effectué, nous avons pris contact avec des autorités de protection des données à caractère personnel et des autorités ayant en charge leur protection – souvent des médiateurs – à l'étranger, afin d'établir une liste de bonnes pratiques. La synthèse de ce tour d'horizon international nous a permis de formuler une proposition adaptable à la Hongrie.

Afin de rendre ce travail opérationnel, nous nous sommes attachés à produire du matériel pédagogique à l'intention des enfants, ainsi qu'une liste à jour d'organismes vers lesquels les victimes peuvent se tourner, ou qui sont susceptibles de mener une action préventive.

Le présent document présente en français les principaux aspects et conclusions de ce travail de recherche, dont il existe une version intégrale en hongrois et en anglais, disponible sur notre site Internet **www.naih.hu** .

Les aspects positifs d'Internet

En Hongrie, les enfants entre 9 et 16 ans passent en moyenne 2,5 heures par jour sur Internet, soit à peu près une journée et demie (39 heures) par mois. Selon une étude réalisée en 2011 par l'Union européenne, 60% de cette tranche d'âge navigue sur Internet quotidiennement, et 35% autre pourcents s'y connectent au moins une fois par semaine[9].



Source : Rapport sur le taux de pénétration d'Internet, 2011/Q3, NRC[10]

Internet représente un avantage considérable pour cette génération, en matière d'accès à l'information et aux savoirs. Il permet également de maintenir le lien social avec des personnes géographiquement éloignées. Depuis 2010, il est devenu la principale source d'information pour les jeunes Américains[11], ce qui est aussi le cas en Hongrie. Les principaux usages d'Internet par le 10-18 ans en Hongrie sont les réseaux sociaux, les loisirs, mais aussi l'apprentissage. L'emploi de moteurs de recherche, ou d'encyclopédies en ligne comme Wikipedia, s'est généralisé comme moyen d'accès privilégié aux connaissances.

9 SÁGVÁRI, Bence, *EU Kids Online*, chapitre sur la Hongrie : http://www.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/hungary.aspx

10 http://nrc.hu/hirek/2012/01/13/Internetpenetracio, 23 avril 2013

11 Pew Research Center study, 4 janvier 2011 : http://mashable.com/2011/01/04/internet-surpasses-television-as-main-news-source-for-young-adults-study/

Le développement de nouvelles formes de culture sur Internet a des conséquences sur les habitudes des enfants, dans tous les domaines de la vie. De nouveaux mots et de nouvelles formes de communication font leur apparition. Ces phénomènes influencent la façon de penser des mineurs tout comme leur comportement. Nous insistons sur l'importance du caractère irrémédiable de cette évolution, et sur le fait qu'il ne s'agit de ne pas y accoler de jugement de valeur.

Les droits des enfants sur Internet

Les droits des enfants sont inscrits dans la Convention relative aux des Droits de l'Enfant, adoptée par l'ONU le 20 novembre 1989, et transposée en droit hongrois par la loi n°LXIV de 1991. Nombre de ses articles sont pertinents dans le contexte d'Internet, et tout particulièrement l'article 16 qui dispose : « 1. Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. 2. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »[12].

Outre le régime juridique général protégeant les mineurs s'applique le droit relatif à la protection des données à caractère personnel. De la même façon que tout autre individu résidant sur le territoire hongrois, ce droit a vocation à protéger les enfants. Cette protection se retrouve même renforcée par la nécessité de recueillir non seulement le consentement de l'enfant mineur de moins de 16 ans pour la collecte de ses données personnelles, mais également celle de ses parents ou de son représentant légal.

Selon la législation hongroise, le traitement de données à caractère personnel doit obéir à plusieurs impératifs. Il doit répondre à un objectif précis et y être proportionnel, limité dans le temps. Les personnes concernées par le traitement doivent avoir donné leur consentement libre et éclairé, et disposent d'un droit d'accès, de rectification et de suppression. Le responsable du traitement s'engage à s'assurer de l'exactitude des données recueillies.

Le principe général selon lequel l'intérêt de l'enfant est supérieur à tout autre intérêt peut en théorie entrer en conflit avec le droit des enfants à une vie privée. Cela se vérifie tout particulièrement dans le cas des procédures de protection de l'enfance au cours desquelles il peut s'avérer nécessaire de collecter et transmettre des renseignements sur les aspects les plus intimes de la vie des enfants. Il en est ainsi par exemple des procédures d'enquête en cas de soupçons de violences parentales. Le fait qu'il s'agisse de données appartenant à des enfants donne également une coloration particulière aux principes généraux de la protection des données, puisque ce qui pouvait paraître légitime comme traitement de données à un âge donné peut ne pas le rester avec le temps[13].

Les cas de commentaires injurieux sur Internet, ou d'abus de données personnelles, posent

[12] Selon une étude de 2012 du Défenseur des droits français (Rapport annuel 2012 consacré aux droits de l'enfant (Enfants et écrans : grandir dans le monde numérique) - Novembre 2012), la diffusion croissante d'Internet et notamment des terminaux mobiles ne saurait être opposée. Les dangers encourus par les enfants sur Internet sont mal connus, et il n'y a pas de stratégie cohérente du législateur pour y faire face. Alors que personne ne met en question les dangers d'un usage excessif de la télévision pour les enfants, le fait de donner des appareils électroniques à ses enfants est aujourd'hui un phénomène de mode. Étant donné que les enfants qui naissent dans l'univers numérique ne font pas la différence entre la vie en ligne et hors ligne, il faut selon le Défenseur des droits interprété l'article 16 de la Convention au sens où il couvre le champ de la vie privée des enfants sur Internet. http://www.defenseurdesdroits.fr/sites/default/files/upload/rapport-droit-enfants-bd-2012.pdf

[13] Working document 1/2008 on the protection of children's personal data

eux aussi des problèmes bien particuliers. Par exemple si les serveurs ne sont pas localisés en Hongrie, la question de la territorialité de loi applicable est complexe à trancher. Il est difficile, bien souvent, de retrouver les fautifs sur Internet. Et lorsque ceux-ci sont identifiés, il est parfois difficile de les punir car ce sont potentiellement eux aussi des enfants. C'est pourquoi la médiation entre les parties, surtout dans les cas de propos injurieux, de diffamation, ou de harcèlement, peuvent se révéler des alternatives efficaces à des procédures juridiques de sanction plus formelles, complexes, longues et coûteuses.

Panorama des principales questions de fond

A. Âge et maturité

Nous désignons ici par le terme d'« enfant » toute personne juridiquement mineure, c'est-à-dire dans le cas de la Hongrie, de moins de 18 ans. La question de la maturité peut être abordée à la fois de façon statique ou dynamique. Il est possible de considérer comme enfant toute personne n'étant pas mûre physiquement et mentalement, mais dont la maturité progresse vers l'état d'adulte. Pourtant il n'est pas certain que, dans la réalité, un jeune adulte de 19 ans soit plus mûr qu'un mineur de 16 ans. La question de la maturité contraint à un examen relatif.

En droit hongrois, l'âge de la responsabilité pénale commence à partir de 12 ans (ce qui peut couvrir des infractions commises en ligne), et celui de la responsabilité civile commence à partir de 16 ans. Dans le cadre de la loi hongroise portant protection des données et liberté de l'information[14], trois étapes sont à distinguer :

- de sa naissance à ses 14 ans, seuls ses parents peuvent donner leur accord pour le traitement des données d'un mineur, après consultation de ce dernier ;
- de 14 à 16 ans, le consentement du mineur concerné comme de ses représentants légaux est nécessaire ;
- à partir de 16 ans, l'enfant mineur, même non-émancipé, peut consentir au traitement de ses données personnelles seul.

Les enfants mineurs peuvent dans tous les cas exercer un droit d'accès à leurs données personnelles, sans, voire contre l'avis, de leurs parents.

L'analyse de la question de l'âge et de la maturité ne serait pas complète sans parler de la question des sites Internet dont l'accès est subordonné à l'âge. Souvent, il s'agit de sites Internet à caractère pornographique, interdit aux mineurs. Il n'est un secret pour personne que les enfants voulant accéder à de tels sites mentent pour y parvenir, et que cela ne nécessite aucune prouesse technique. D'autres sites sont également concernés : selon Consumer Reports, 5 millions des utilisateurs inscrits sur Facebook sont des mineurs de moins de 10 ans, malgré la limite d'âge inférieur fixée à 13 ans par ce réseau social[15].

B. La question de l'anonymat : est-ce plus facile avec un masque ?

Nombre d'internautes se créent une identité virtuelle en ligne, construite autour d'un pseudonyme. L'objectif est alors de bénéficier d'un certain degré d'anonymat sur les blogs, forums et dans les commentaires publiés, alors même qu'un même individu est capable de publier sous son nom une quantité similaire de données personnelles, sous son vrai nom, sur des réseaux sociaux.

Cet anonymat permet bien souvent de se cacher, et de nombreux cas d'abus se présentent, des internautes commettant des infractions sous le couvert d'une identité virtuelle. La Corée du Sud

[14] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról1

[15] Http://index.hu/tech/2013/04/22/gyerekek_es_az_internet/

a ainsi interdit cette pratique du pseudonymat dans un but de maintien de l'ordre, et cette question a également été étudiée dans d'autres pays, dont la France. Il y a malgré tout de bonnes raisons de considérer que la volonté d'interdire cet anonymat sur Internet soit politique et économique plutôt que juridique : il est plus facile de centraliser des données personnelles autour d'une identité réelle que d'une ou plusieurs identités virtuelles, ce qui améliore par exemple la capacité des entreprises à faire du marketing ciblé. Ces arguments ont conduit le Comité des Ministres du Conseil de l'Europe a adopté en 2003 une déclaration affirmant notamment que : « Afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les Etats membres devraient respecter la volonté des usagers de l'Internet de ne pas révéler leur identité »[16].

C. Troubles de la personnalité

La psychologie et la psychiatrie s'intéressent depuis les années 1990 aux troubles de la personnalité pouvant résulter d'une utilisation pathologique des nouvelles technologies, notamment d'Internet. Si Internet est à bien des égards un atout indéniable, sa mauvaise utilisation, ou son utilisation abusive, peuvent entraîner des troubles psychologiques durables, parmi lesquels :

- les troubles de la personnalité (pouvant être liés à l'usage d'identités virtuelles) ;
- le développement de comportements pathologiques en ligne ;
- le développement de comportements addictifs ;
- l'interaction comorbide avec des troubles psychologiques ou psychiatriques pré-existants.

Les symptômes de troubles de la personnalité directement imputables à Internet sont les suivants :

- Le temps passé devant l'ordinateur ;
- L'évolution des relations interpersonnelles menant à une distanciation de ses proches de la « vie réelle ;
- L'immersion dans un espace et un temps virtuel, aboutissant à une perte de contact avec l'expérience vécue du « monde réel » et de ses enjeux ;
- L'impossibilité de traiter certains contenus (par exemple violents ou à connotation sexuelle), entraînant des réactions pathologiques et des troubles de la socialisation ;
- La transformation de la communication, notamment son appauvrissement : dégradation de la parole, transformation de la méta-communication, diminution de la capacité à analyser les signaux corporels et sémiotiques, incapacité à percevoir les émotions d'autrui ;
- En conséquence des éléments indiqués ci-dessus : développement de troubles anxieux et de l'isolement.

Que pouvons-nous faire face à de tels symptômes ?

- Inciter les parents et l'entourage des enfants à la vigilance vis-à-vis des habitudes des enfants sur Internet ;
- Mise en place de limites horaires pour l'accès à certains terminaux ;
- Expliquer aux enfants d'une façon adaptée à leur âge et à leur maturité les règles et les possibilités ;
- Avertir les enfants des éventuels dangers ;

[16] https://wcd.coe.int/ViewDoc.jsp?Ref=Decl-28.05.2003&Language=lanFrench&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864

- Inciter l'enfant de façon positive à des programmes et occupations alternatifs à l'informatique ;
- Dans les cas graves, envisager une psychothérapie familiale ou pour l'enfant.

Sur ces aspects psychologiques, nous avions conclu dans notre étude qu'une utilisation consciente et opportune d'Internet permettait d'éviter nombre de ces pathologies. Les pathologies liées à l'emploi d'Internet révèlent et renforcent souvent des problèmes pré-existants. L'essentiel des symptômes convergent vers des troubles anxiogènes et l'isolement social. Les comportements pathologiques et déviants s'auto-renforcent mutuellement. Une coordination pluri-disciplinaire est pertinente en vue de la résolution de ces problèmes. Il est également important de rappeler, qu'en cas de trouble grave, l'aide d'un professionnel est incontournable !

D. Espaces publics, amis inconnus

Par l'incroyable rapidité de leur développement et leur impact sur nos vies privées, les communautés et les virtuelles sont un des phénomènes les plus marquants d'Internet. Les critères qui permettent de définir un réseau social sont les suivants :

- Les utilisateurs peuvent créer des profils publics ou semi-publics ;
- Les utilisateurs peuvent se connecter entre eux ;
- Les utilisateurs peuvent connaître les réseaux de contacts d'autres utilisateurs.

Le premier réseau social, classmates.com, est né en 1995 aux États-Unis. Aujourd'hui, avec son milliard d'utilisateurs inscrits en 2012, Facebook est sans conteste et de très loin le plus populaire d'entre eux. La mise en ligne de millions de profils, souvent accessibles publiquement, fragilise la sphère privée de générations entières, et en particulier celle des jeunes. Elle offre par ailleurs un terreau favorable aux abus en ligne tels le *sexting*, le *grooming* et le harcèlement.

Selon une enquête réalisée au niveau européen[17], 38% des 9-12 ans et 76% des 13-16 ans sont inscrits sur Facebook. Leur comportement se caractérise par un niveau certain d'imprudence : seuls 16% des utilisateurs hongrois de Facebook entre 9 et 16 ans ont limité l'accès à leur profil au seul cercle de leurs amis[18].

La disponibilité publique d'informations personnelles sur Internet fait courir le risque aux individus concernés de la dispersion de ces données, et partant, de leur réutilisation à des fins pour lesquelles elles n'étaient pas prévues, susceptibles de porter préjudice. Le scandale de l'affaire Prism, qui a éclaté en 2013, illustre ce problème, les services secrets américains ayant collecté et traité les données personnelles de millions de personnes, que celles-ci avaient elles-mêmes mis en ligne sur Internet. Une fois que les données sont copiées sur un support qui n'appartient pas au contrôleur de données à qui celles-ci avaient été originellement confiées, les différents droits dont les individus concernés bénéficient, comme le droit d'accès, deviennent difficiles voire impossibles à exercer. L'effacement intégral et définitif d'une donnée sur Internet n'est jamais garanti.

---

[17] LIVINGSTONE, Sonia, OLAFSSON, Kjartan et STAKSRUD, Elisabeth, *EU Kids Online – Social Networking, Age and Privacy*, 2011, disponible en ligne : http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf

[18] SÁGVÁRI, Bence, *EU Kids Online*, chapitre sur la Hongrie : http://www.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/hungary.aspx

Enfin, il faut évoquer au sujet des réseaux sociaux la possibilité que des tiers publient des données personnelles reliées à une personne, par exemple par le système de « tags » (étiquettes) applicables aux photos sur Facebook. La mise en ligne de données appartenant à autrui a été le sujet d'une affaire traitée par la Cour de justice de l'Union européenne (CJUE) : l'affaire Lindqvist[19]. Dans celle-ci, une personne avait, de bonne foi, mis en ligne sans leur consentement les coordonnées de bénévoles travaillant pour le compte d'une association cultuelle, ce qui est bien entendu contraire à la directive européenne de protection des données personnelles n°95/46/CE.

E. Les contenus nuisibles

De nombreux contenus disponibles sur Internet peuvent, bien qu'ils ne soient pas nécessairement illégaux en soi, porter préjudice au développement de l'enfant. Typiquement, il s'agit de contenus violents, pornographiques, faisant l'apologie du suicide ou de la consommation de drogues. L'accès à ces contenus est très souvent involontaire, et apparaît par exemple dans des résultats de recherches effectuées sur la base de mots-clefs *a priori* inoffensifs, ou encore par le biais de fenêtres intempestives et de courriers indésirables.

Nous avons passé en revue dans notre étude trois types de solutions :

- Tout d'abord, l'éducation par les adultes, qui doivent préparer les enfants au fait que même involontairement, ils peuvent être amenés au cours de leur navigation sur Internet à tomber sur des contenus indésirables, voire nocifs. Il est important d'éveiller l'esprit critique des enfants face à ces contenus, et de leur permettre d'en parler à un adulte de confiance sans crainte d'être punis ;
- La deuxième solution consiste à mettre en place un système de contrôle parental ;
- Certains pays mettent en œuvre des systèmes centraux de censure d'Internet. Cette censure peut avoir des motifs politiques, comme en Chine, mais certains États démocratiques mettent en œuvre les mêmes techniques pour censurer certains types de contenus illégaux. Ainsi, l'Allemagne censure les contenus négationnistes, et la Norvège les contenu pédopornographiques. Depuis 2012, le juge hongrois peut ordonner la censure d'une ressource web qui est l'objet d'un délit, qui est l'outil d'un délit, ou qui est le résultat d'un délit[20]. L'adoption de cette nouvelle disposition du Code pénal hongrois était justifiée par la lutte contre la pédophilie en ligne et la transposition de l'article 25 de la directive 2011/93/UE[21].

F. Tendances prévisionnelles

Les cinq sous-chapitres précédents dressent un panorama sommaire des problèmes déjà bien ancrés auxquels les enfants font face sur Internet. Nous avons également tenu à analyser brièvement les nouvelles tendances qui se dégagent et auxquelles nous devons faire face.

1. <u>L'Internet ubiquitaire, ou Internet des objets</u>

[19] CJUE 6 novembre 2003, Aff. C-101/01 « Lindqvist » Rec. I-12992
[20] Article 77 du Code Pénal hongrois
[21] Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie JO 17/12/2011

À l'origine, l'accès à Internet passait impérativement par un ordinateur de bureau. Aujourd'hui se développent une quantité de terminaux sous formes d'objets du quotidien : dès aujourd'hui, les téléphones et les tablettes permettent un accès à Internet où que l'on se trouve, et déjà se développent les lunettes intelligentes, montres intelligentes, et autres objets connectés, comme les réfrigérateurs. Dotés parfois de capteurs divers (antenne GPS permettant la géolocalisation, accéléromètre…), ces objets sont connectés en permanence et transmettent une quantité exponentielle de données personnelles. Se développent de surcroît des phénomènes de mode chez les jeunes générations qui les poussent à adopter massivement ce type d'objets.

2. Le « Big Data »

Toutes ces données évoquées ci-dessus sont généralement centralisées par de grandes multinationales qui disposent ainsi de volumes astronomiques de données personnelles de nature variée, nourrissant des algorithmes complexes qui permettent de les traiter avec le plus de vitesse possible. Ces trois « V » (volume, variété et vitesse) définissent ensemble la notion de « Big Data ». Cette technique pourra vraisemblablement permettre de prévoir le comportement des usagers, ce qui constitue un nouvel enjeu de taille pour la protection de la vie privée. Cette collecte de données est d'ores et déjà facilitée par la mise à disposition d'applications toujours plus nombreuses permettant de partager instantanément des contenus comme des vidéos ou des photos à partir de terminaux mobiles. D'autres applications, disponibles sur *smartphones*, obtiennent l'accès aux données stockées sur ces derniers, comme les carnets d'adresses, et les transmettent à l'éditeur du logiciel.

Ces enjeux posent des questions nouvelles auxquelles nous ne savons pas encore bien quelles réponses donner. Ils visent particulièrement les enfants, puisqu'ils sont la cible privilégiée des entreprises proposant les services et applications décrites dans ce chapitre.

Panorama des principales déviances sur Internet

A. Le harcèlement sur Internet

Le harcèlement est le principal facteur de risque auxquels sont confrontés les jeunes de 10 à 16 ans sur Internet. Ses motifs sont toujours personnels, et le coupable « torture » souvent sa victime sur une durée longue et répétée. La principale caractéristique de ces actes sont la vexation et l'injure, cependant le mode opératoire peut varier : il peut s'agir d'envois à répétition, jour et nuit, de courriers électroniques menaçants, de messages diffamatoires postés sur des réseaux sociaux, ou encore de commentaires injurieux sur le blog de la victime. Le harcèlement en ligne se prolonge dans la grande majorité des cas dans la vie réelle. Les auteurs sont en général d'autres enfants, appartenant à l'entourage de la victime. La possibilité d'anonymat qu'offre Internet confère au coupable un sentiment d'impunité, et alourdit dans ce cas la portée psychologique de l'acte sur la victime. Un autre facteur aggravant est que le harcèlement en ligne n'offre pas, à l'instar du harcèlement à l'école par exemple le répit constitué pour la victime par le fait de rentrer chez elle après les cours.

Un exemple illustrant les phénomènes décrits ci-dessus est le suicide aux États-Unis d'une fille en 2006. Dans cette affaire, une mère et sa fille se faisaient passer pour un garçon de 16 ans, et échangées des e-mails avec la victime sous cette fausse identité. L'affaire avait été médiatisée parce que dans un premier temps, le parquet n'était pas parvenu à identifier de chef d'accusation dans la loi qui puisse s'appliquer au cas d'espèce.

B. Le phénomène des mèmes

La diffusion de messages sur Internet ne concerne pas uniquement la diffusion publicitaire. Un grand nombre d'informations diffusées relèvent des rumeurs, de vidéos et images gênantes, qui peuvent être le fruit d'une expression artistique et prêter à sourire, mais qui souvent débouchent sur de véritables campagnes de diffamation. La différence entre le harcèlement en ligne et l'envoi de mèmes est qu'en règle général, l'auteur et la victime ne se connaissent pas personnellement. Cette dernière est en général quelqu'un de potentiellement inconnu, que les internautes

Ce sont généralement de personnes célèbres qui sont représentées dans les mèmes, comme le pape Benoît XVI suite à sa démission. Dans de rares cas cependant, il peut s'agir de personnes privées et même de mineurs. C'est ce qui est arrivé à une jeune fille de 11 ans en Californie, qui partagea des vidéos d'elle sur Youtube où elle discutait de ses goûts musicaux. Rapidement, des rumeurs se sont mises à circuler à son sujet sur Internet, et elle devint avec sa famille victime de harcèlement. La victime est aujourd'hui toujours sous traitement psychiatrique suite au traumatisme subi au cours de cet épisode[22].

[22] Http://knowyourmeme.com/memes/events/jessi-slaughter

C. Les trolls

L'argot d'Internet définit les « trolls » comme étant des personnes qui bombardent un fil de discussion de messages provocants et agressifs, voire injurieux, dans le but de susciter une réaction vive et de déranger la discussion en cours. Le dicton anglais « Do Not Feed the Troll », soit « ne nourris par le troll », se réfère à ce type de comportement et incite à ne pas réagir à la provocation.

D. L'envoi d'images de nature sexuelle (*sexting*)

Le mot-valise anglais « Sexting » s'emploie pour désigner l'envoi d'images ou de vidéos érotiques par les moyens de communication modernes. Cette pratique a gagné en popularité parmi les jeunes ces dernières années.

> « Les résultats d'une étude américaine menée en 2008 sur l'ensemble du territoire et visant à prévenir les cas de grossesse involontaire chez les jeunes, ont montré que 20% des jeunes entre 13 et 19 ans envoient des images nues ou à moitié nues d'eux-même. 25% des filles et 3% des garçons ont répondu par l'affirmative à la question visant à savoir s'ils avaient déjà reçu une image érotique qui ne leur était initialement pas destinée. […] »[23]

Ces chiffres soulignent la prévalence du phénomène auprès des jeunes. La difficulté d'appréhension de ce phénomène est accrue par le fait que dans l'essentiel des cas, les images sont produites avec le consentement et la participation active du modèle de la photo. Une fois que l'image prise et mise en ligne, le fichier suit sa propre vie et il devient impossible d'en contrôler la diffusion, ce qui entraîne de nombreux cas d'abus graves.

E. La pédophilie sur Internet

Un pédophile est un adulte sexuellement attiré par les enfants. L'opinion publique réprouve avec vigueur la pédophilie, et ses manifestations sont réprimées par le droit pénal. C'est pour cette raison que les criminels pédophiles cherchent à masquer leur activité. À cet égard, Internet leur offre un terrain idéal leur garantissant une certaine forme d'anonymat. La pédophilie en ligne recouvre non seulement des actes commis par des individus isolés mais aussi les activités du crime organisé. L'acquisition et la diffusion d'images pédopornographiques est nettement plus aisée sur Internet. Voici un exemple banal : un quarantenaire s'inscrit sur un réseau social en prétendant avoir 18 ans, met en ligne des photos attirantes «de lui», entame une discussion avec des adolescentes, et suscite leur confiance au point que ces dernières deviennent susceptibles de lui envoyer des photos d'elles déshabillées.

Du point de vue du droit de la protection des données personnelles, la procédure est complexifiée par le fait que souvent, la victime participe et facilite le travail du pédophile en mettant elle même en ligne les images incriminées. De plus, les images sont stockées sous un format visant à rendre plus difficile l'identification de la victime – notamment en remplaçant la tête de la victime par celle d'une tierce personne.

[23] Zoltán Szathmáry: Criminality in the information society, Constitutional criminal dilemmas in the information society, PhD thesis, Budapest 2012. p. 69.

F. Infiltration et fausse identité (*grooming*)

Le terme anglais de «grooming», pour lequel il n'existe pas d'équivalent en hongrois, désigne dans le cadre d'Internet le fait pour une personne de s'infiltrer dans un groupe ou d'acquérir la confiance d'une personne en donnant de fausses informations sur soi, visant à se faire passer pour autre chose que ce que l'on est. Typiquement, il s'agit de comportements de trentenaires et de quarantenaires, inscrits sur les réseaux sociaux, et se faisant passer pour des adolescents. Pour l'essentiel, il s'agit de personnes prêtes à traquer leurs victimes pendant des mois, sur la base d'une stratégie planifiée visant à obtenir leur confiance pour obtenir des images pédopornographiques, de les faire participer à des activités sexuelles ou de les rencontrer physiquement. Les enfants ne se rendent compte souvent que trop tard de supercherie, et en raison de la honte qu'ils ressentent à s'être faits ainsi duper, il est rare qu'ils demandent l'aide d'un adulte.

G. Les jeux en ligne destinés aux enfants

La littérature scientifique sur le sujet ne prend aujourd'hui en compte comme pathologie que l'addiction aux jeux de hasard, et pas celle aux jeux vidéos. Cette dernière est plutôt considérée comme un symptôme[24].

La question des jeux de hasard est simple à trancher d'un point de vue juridique : l'article 1-6 de la loi XXXIV de 1991 portant réglementation des jeux de hasard interdit formellement la participation des mineurs à ces jeux.

Le jeu – y compris le jeu vidéo – est une activité ludique qui dans bien des cas contribue au développement équilibré de l'enfant. Les jeux en ligne peuvent même offrir des situations de mise en pratique et d'accumulation de connaissances. Il faut cependant prendre en considération les potentiels effets négatifs. Premièrement, l'intérêt principal des producteurs de jeux vidéos réside dans la réalisation de profits. Cet objectif peut être (légalement) atteint en mettant sur le marché des jeux de plus en plus chers, en encourageant les consommateurs à acquérir des contenus supplémentaires et en tentant de conserver la fidélité du joueur le plus longtemps possible.

De plus en plus de jeux théoriquement gratuits dysfonctionnent ou offrent une expérience de jeu pénible tant que le joueur n'achète pas d'« accessoires » payants. En 2011, en Allemagne, les consommateurs ont dépensé 233 millions euros pour de tels contenus, soit 100 millions de plus que l'année précédente[25].

L'achat de ces composants est très facile : il peut s'effectuer par exemple en appelant un numéro de téléphone ou en envoyant un SMS surtaxé. Les enfants utilisent souvent le téléphone de leurs parents pour effectuer ce genre d'achat. Même si les administrateurs de sites Internet promettent de limiter l'achat de composants à un nombre limité d'hypothèses, ils ne respectent généralement pas leurs engagements. De plus, les joueurs sont incités à rester dans le jeu par des mécanismes de sanction. Ceux qui « quittent » un jeu de façon prématurée peuvent être exclus pour

[24] Andrea Vida: Impact of information and communication culture on teenagers from: http://xenon.bibl.u-szeged.hu/~vidaa/holi/03/szenvbet/vidaa.pdf 24-03-2013

[25] In der Kostenfalle – Kinderspiele im Internet, Sendung vom 11. Dezember 2012, http://www.zdf.de/ZDFmediathek/beitrag/video/1794584/#/beitrag/video/1794584/Kostenfalle-Kinderspiele-im-Internet, 08-03-2013

une durée allant de quelques heures à quelques semaines, ce qui a des conséquences financières lourdes sur les investissements qu'ils ont consenti dans le cadre du jeu.

Les jeux en ligne, sur PC, console ou smartphone, peuvent être joués par plusieurs personnes en même temps. Une des catégories de jeux vidéos parmi les plus populaires chez les enfants hongrois sont les jeux de rôle en ligne massivement multi-joueurs connus sous leur acronyme anglais de MMORPG. Ces jeux, d'une façon similaire aux réseaux sociaux, permet aux joueurs d'avoir accès aux données personnelles d'autres joueurs et d'échanger entre avec eux. C'est pourquoi cette catégorie de jeux soulève des questions particulières en termes de protection des données. Il est conseillable de lire leur politique de confidentialité avant de s'y inscrire. Les données qu'ils récoltent concernent généralement un nom d'utilisateur, une adresse mail, et la date de naissance. Des données géographiques sont également traitées afin de déterminer le serveur de jeu et les joueurs les plus proches physiquement. Lorsqu'un âge minimal s'applique au jeu, un système de confirmation de l'âge peut également être mis en œuvre.

Cela peut paraître étonnant mais la protection la plus efficace pour les jeux en ligne est de faire en sorte que l'enfant puisse jouer avec ses parents ou que toute la famille s'inscrive et joue[26].

H. Autre formes d'abus en relation avec la protection des données personnelles

Internet est devenu intimement lié à notre vie quotidienne. Nous y passons désormais un temps significatif de notre vie. Bon nombre des services qui y sont disponibles sont à première vue gratuit ; mais cette gratuité cache bien souvent des modèles économiques fondés sur la monétisation des données personnelles des utilisateurs inscrits. Selon l'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA), lorsqu'ils ont le choix entre plusieurs services à prix équivalent, les consommateurs tendent à préférer celui offrant les meilleures conditions de confidentialité. Mais lorsqu'il y a une différence de prix, ils choisissent toujours le service le moins cher, sans prendre en considération les arguments relatifs à la protection des données personnelles.

La collecte déloyale de données, telle que réprimée par le Code pénal hongrois, peut servir, outre à des tentatives de « phishing » (piratage des données bancaires), au harcèlement, à la diffamation, au chantage ou à l'usurpation d'identité de la victime.

Un autre problème est constitué par le fait que nombre de sites contiennent des passerelles vers d'autres, par exemple avec la technique du XSS ou Cross Site Scripting. Or, cela peut engendrer des failles de sécurité favorisant la diffusion de logiciels espions. La multiplication de l'imbrication de sites entre eux est une circonstance qui aggrave ce risque considérablement.

Enfin, une dernière catégorie de services en ligne faisant peser des doutes quant à leur conformité avec les règles de la protection des données à caractère personnel sont les sites de vente en ligne. Il arrive par exemple que des enfants enchérissent avec le compte de leurs parents, à l'insu de ces derniers. Ces cas parviennent alors au service client de ces sites. L'inscription des enfants est normalement interdite sur ces sites, mais ils ne disposent pas des moyens nécessaires à la vérification de la limite d'âge inférieur. Il existe aussi des cas de fraude en ligne, où le vendeur collecte l'argent pour des biens inexistants, qu'il ne peut donc pas expédier à l'acquéreur[27].

---

[26] http://mediasmarts.ca/blog/game-tips-parents 15 avril 2013

[27] http://www.penzcentrum.hu/vasarlas/tizezreket_bukhatnak_a_gyanutlan_vasarlok_tamadnak_az_atveros_netes_boltok.1035976.html ,15 mai 2013

Panorama des bonnes pratiques à l'international

A. Portugal. Projet « DADUS »

En 2008, l'autorité portugaise de protection des données a proposé l'introduction du thème des données personnelles dans les programmes d'enseignement scolaire. La première phase de ce projet de long-terme, appelé « Projet Dadus » et destiné aux enfants de 10 à 15 ans, a été élaborée avec le soutien du Ministère de l'Éducation. Il est divisé en unités thématiques et comprend à la fois un volet destiné aux enfants et un volet destiné au personnel enseignant.

Un site Internet (http://dadus.cnpd.pt) a été mis en ligne. Il contient du matériel pédagogique téléchargeable par les enseignants ainsi qu'un contenu vidéoludique pour les enfants. Depuis le 28 janvier 2008, de nombreux événements locaux et nationaux ont servi à diffuser l'information au Portugal. Plus de 1400 enseignants se sont inscrits sur le site Internet, signe du succès de l'initiative.

Reconnaissant l'importance du sujet et le succès du projet, le Ministère de l'Éducation a introduit en 2012 la question des données personnelles dans le programme national d'éducation aux TIC à destination des collégiens.

Plus d'informations : http://dadus.cnpd.pt

B. Irlande. Projet « Private I, Public Eye »

L'autorité irlandaise de protection des données a placé la question de la jeunesse parmi ses priorités[28]. Plusieurs initiatives ont été menées à ce sujet, parmi lesquelles :

- Le CSPE Resource Booklet (un manuel en couleurs de 92 pages) ;
- Un concours de vidéos, disponible sur www.youtube.com/dataprotection ;
- L'enquête « Young Social Innovators » de 2008 ;
- L'enquête sur la vie privée de 2010 intitulée « The I in Online » ;
- La publication d'un guide parental sur la sécurité sur Internet par le *Office for Internet Safety* ;
- Le Médiateur irlandais des enfants a organisé une consultation nationale sur le thème du harcèlement à l'école et en ligne, qui touchent en Irlande autour du quart des écoliers du primaire. L'étude est disponible en ligne : http://www.oco.ie/assets/files/OCO-Bullying-Report-2012.pdf ;
- Une agence de communication irlandaise, Fuzion Communications, a lancé une campagne d'information graphique destinée aux enfants sur les réseaux sociaux : http://www.thejournal.ie/safebook-how-to-stay-safe-

[28] http://dataprotection.ie/viewdoc.asp?docID=520

online-657753-Nov2012/

C. Écosse. Projet « Respect Me »

Ce projet, initié par le gouvernement écossais, a été mené par le centre de lutte contre le harcèlement de Trinity College, en collaboration avec le Médiateur écossais des enfants. D'autres associations partenaires y ont contribué. Il s'agit principalement d'un programme de formation et de sensibilisation aux problèmes du harcèlement des enfants.

Plus d'informations : http://www.respectme.org.uk/What-do-I-do-if-a-child-tells-me-they-are-being-cyberbullied.html

D. Norvège. Projet « You Decide »

Le Projet « You Decide » a été conduit par un partenariat entre le Conseil Norvégien de la Technologie, l'Inspection Norvégienne des Données Personnelles et le Centre pour l'éducation aux NTIC. L'objectif est de sensibiliser les enfants aux enjeux de la protection des données personnelles. Deux volets sont compris dans ce projet : un destiné aux élèves du primaire, et l'autre aux collégiens. Chaque paquet contient de la documentation, et une liste de tâches et sujets à débattre. Des vidéos ont été produites dans la vocation d'être diffusées en classe et de susciter la discussion entre les élèves.

Plus d'informations :
http://dubestemmer.no/en/About_You_Decide/#content

E. Nouvelle-Zélande : « Youth Privacy Kit »

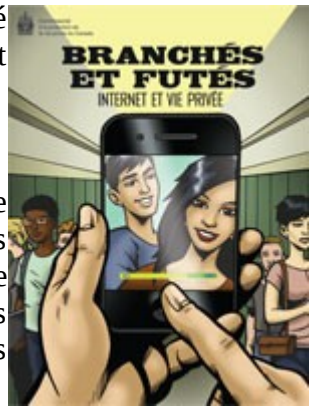
YOUTH PRIVACY

En 2009, le Commissaire néo-zélandais à la protection des données a démarré un projet visant à comprendre la façon dont les jeunes conçoivent la notion de vie privée, et par suite, à faire produire par des jeunes du matériel pédagogique sur le sujet. Le projet a été conduit par un groupe de travail de quinze collégiens. Les trois sujets prioritaires qui se sont démarqués des travaux sont : l'information, le consentement et l'usage approprié des données personnelles. Le groupe de travail a émis l'avis selon lequel le moyen le plus efficace de sensibiliser leur tranche d'âge serait de faire réaliser aux collégiens de exposés en classe sur le sujet.

Le « Youth Privacy Kit » développé inclut les éléments suivants : des fiches sur la protection des données, des histoires relatant des exemples concrets, une courte vidéo d'introduction du sujet, un guide d'activités, un quiz, des posters etc…

Plus d'informations : www.privacy.org.nz/youth

F. Canada : bandes dessinées et conseils



Le Commissariat à la protection de la vie privée du Canada a développé des outils à destination des parents et du personnel éducatif concernant disponibles à l'adresse : http://www.priv.gc.ca/youth-jeunes/index_f.asp .

Une bande dessinée romanesque en couleur destinée aux enfants, que nous avons traduite en hongrois, illustre aux enfants la facilité avec laquelle nos données personnelles peuvent être échangées sur Internet. Cette bande dessinée narre les mésaventures en ligne d'un frère et d'une sœur, aux prises avec les difficultés de protéger efficacement ses données sur Internet et avec des objets connectés.

G. États-Unis d'Amérique

En 1998, le Congrès américain a adopté le Children's Online Privacy Act (COPPA)[29], qui prévoit un renforcement des obligations pesant sur les contrôleurs de données personnelles qui se rapportent à des mineurs. Au titre des dispositions clefs de cette loi figurent l'obligation de recueillir le consentement actif (*opt-in*) des représentants légaux des enfants de moins de 13 ans pour le traitement de leurs données personnelles et l'obligation pour le contrôleur de participer à des séances de formation sur les données personnelles. Le contrôle du respect de ces dispositions est confié à la Federal Trade Commission. Une enquête récente a démontré que l'essentiel des applications pour téléphone portable destinées à des enfants ne respectait pas les dispositions de la loi et transmettait notamment à des tiers des données sur le comportement de ceux-ci, à leur insu et bien évidemment sans le consentement de leurs représentants légaux[30].

[29] Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2581-728, enacted October 21, 1998).

[30] http://www.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing

H. Union européenne

Le programme « Safer Internet » regroupe sous la tutelle de l'Union européenne des organisations nationales engagées dans la protection de l'enfance. L'un des objectifs est de permettre l'accès à des centres d'appel proposent une aide et des informations. Le 5 février est la Journée mondiale pour un Internet plus sûr[31].

L'enquête « EU Kids Online » regroupe des étude menées dans les États membres de l'Union européenne. Elle est disponible sur le site Internet suivant : www.eukidsonline.net .

[31] www.saferinternet.hu

La recette hongroise

L'objectif de notre étude n'était pas simplement théorique. Elle nous a servi à développer nos propres outils pédagogiques de sensibilisation à la protection des données personnelles.

Nous souhaitons promouvoir quelques initiatives et idées simples, peu coûteuses et inspirées des pratiques internationales, qui pourraient selon nous sensibiliser un public intéressé d'adultes et d'enfants à une utilisation d'Internet plus sophistiquée et plus respectueuse des autres usagers.

Histoires

Les élèves d'une classe ou d'un groupe plus restreint lisent ou bien mettent en scène des histoires vraies ou fictives impliquant une infraction au droit à la vie privée. Ils discutent ensuite les problèmes soulevés par la trame narrative depuis différents points de vue. Il s'agit de faire de la pédagogie par le jeu dramatique. La discussion est portée par l'intervenant sur l'analyse du comportement des protagonistes, pour amener les participants à se demander comment ils auraient pu, à leur place, éviter la mise en danger de leurs propres données personnelles.

Journal de bord de la vie privée

Chaque élève se voit confier la tâche de tenir pendant une courte période variant d'une semaine à un mois un journal comportant les informations suivantes :

- Dans quelle mesure a-t-il rendu publiques des données concernant sa vie privée ?
- Qu'est-ce que des tiers (personnes connues comme inconnues) ont écrit ou dit à propos de lui ?
- A-t-il révélé son nom, son numéro de téléphone ou son adresse e-mail à qui que ce soit sur Internet ?
- Se sont-ils inscrits à un site web ?
- Ont-ils téléchargé ou téléversé des fichiers ?
- Ont-ils utilisé des applications pour smartphone ?
- Etc…

Une fois le journal écrit, la classe ou le groupe est invité à discuter librement de ce qui ressort de cette expérience.

Dresser le portrait d'un tiers

En utilisant ces journaux de bord et les données librement accessibles sur Internet, il est demandé aux participants de dresser le profil d'une personne et de se poser la question de la mesure dans laquelle le profil ainsi dressé correspond à la personne dans la réalité.

Un second exercice consiste à demander aux enfants de désigner un proche (parent, camarade de classe…), puis de le confronter au profil dressé grâce à l'ensemble des informations librement disponibles en ligne sur celui-ci. Ses réactions sont ensuite analysées, et l'enfant sera amené à se poser la question de s'il y a des données concernant sa vie privée qui bien que mises en ligne concernent des éléments que la personne concernée aurait préféré garder pour soi.

Œuvres artistiques traitant d'infractions graves au droit à la vie privée et pouvant servir à la

sensibilisation aux problématiques de la protection des données à caractère personnel

Films

- *Traque sur Internet*, de Irwin Winkler, 1995 (titre original : *The Net*)
- *The Game*, de David Fincher (1997)
- *La vie des autres*, de Florian Henckel von Donnersmarck (2006) (titre original : *Das Leben der Anderen*)
- *Trust*, de David Schwimmer (2010)
- *Le mur de l'humiliation*, de Charles Binammé (2011) (titre original : *Cyberbully*)
- *Caught in the web*, de Chen Kaige (2012)

Romans

- *1984*, de George Orwell
- *L'Honneur perdu de Katharina Blum*, de Heinrich Böll
- *Sa Majesté des mouches*, de William Golding
- *3 096 jours : comment j'ai survécu en captivité pendant huit ans et demi*, de Natascha Kampusch

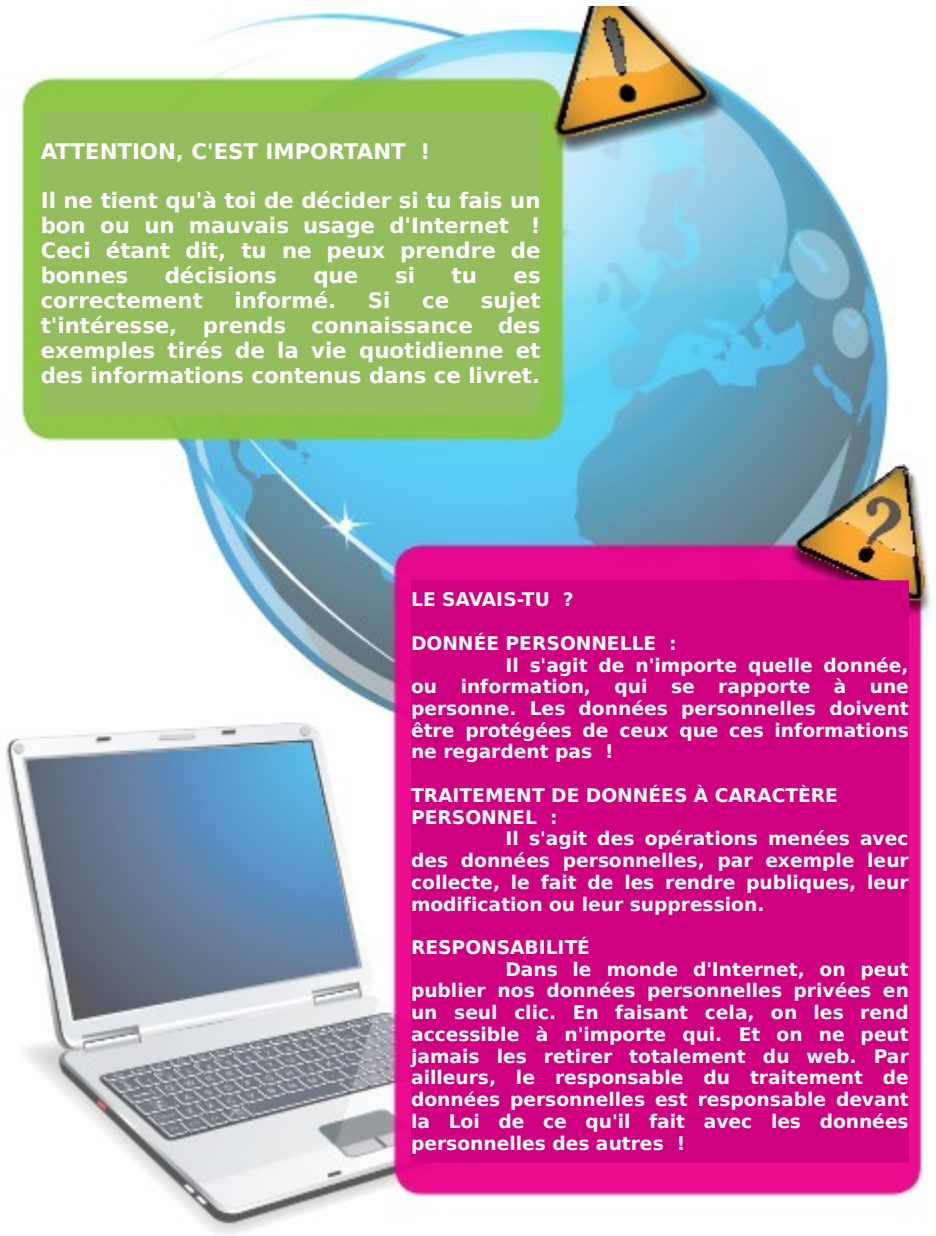
Poèmes

- *De l'air !*, de Attila József (titre original : *Levegőt!*)
- *On m'a inscrit dans toutes sortes de livres* de Dezső Kosztolányi (titre original : *Beírtak engem mindenféle könyvbe*, disponible en anglais sous le titre de : *Laments of a sorrowful man*)
- *Une phrase sur la tyrannie* de Gyulla Illyés (titre original : *Egy mondat a zsarnokságról*)

ANNEXES

Livret d'information de l'Autorité hongroise de protection des données
sur l'usage conscient d'Internet à destination des enfants

(*Ceci n'est qu'un extrait du document hongrois, dont une traduction intégrale en anglais est disponible sur notre site Internet* www.naih.hu)



ATTENTION, C'EST IMPORTANT !

Il ne tient qu'à toi de décider si tu fais un bon ou un mauvais usage d'Internet ! Ceci étant dit, tu ne peux prendre de bonnes décisions que si tu es correctement informé. Si ce sujet t'intéresse, prends connaissance des exemples tirés de la vie quotidienne et des informations contenus dans ce livret.

LE SAVAIS-TU ?

DONNÉE PERSONNELLE :
Il s'agit de n'importe quelle donnée, ou information, qui se rapporte à une personne. Les données personnelles doivent être protégées de ceux que ces informations ne regardent pas !

TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL :
Il s'agit des opérations menées avec des données personnelles, par exemple leur collecte, le fait de les rendre publiques, leur modification ou leur suppression.

RESPONSABILITÉ
Dans le monde d'Internet, on peut publier nos données personnelles privées en un seul clic. En faisant cela, on les rend accessible à n'importe qui. Et on ne peut jamais les retirer totalement du web. Par ailleurs, le responsable du traitement de données personnelles est responsable devant la Loi de ce qu'il fait avec les données personnelles des autres !

Glossaire Internet

Bannir

Action consistant à interdire l'accès d'un canal de discussion à une ou plusieurs personnes. Une personne bannie ne peut plus y accéder, même si elle change de pseudo.

Bannière

Banderole à caractère publicitaire présente sur un grand nombre de sites. Il s'agit de la méthode la plus courante de faire de la publicité sur Internet.

Botnet

Réseau de « robots ». Les botnets connectent entre eux des ordinateurs zombis, contaminés par des virus et des logiciels espions permettant à un pirate d'entre prendre le contrôle à distance. Le pirate peut utiliser à ses propres fins la puissance de calcul de l'ordinateur contaminé. En général, le propriétaire de ce dernier ne s'en rend pas compte. Ces réseaux sont souvent utilisés pour l'envoi de spams. Ils sont capables d'en générer jusqu'à 25 000 par heure. Ils peuvent être utilisés dans d'autres buts criminels.

Tchat

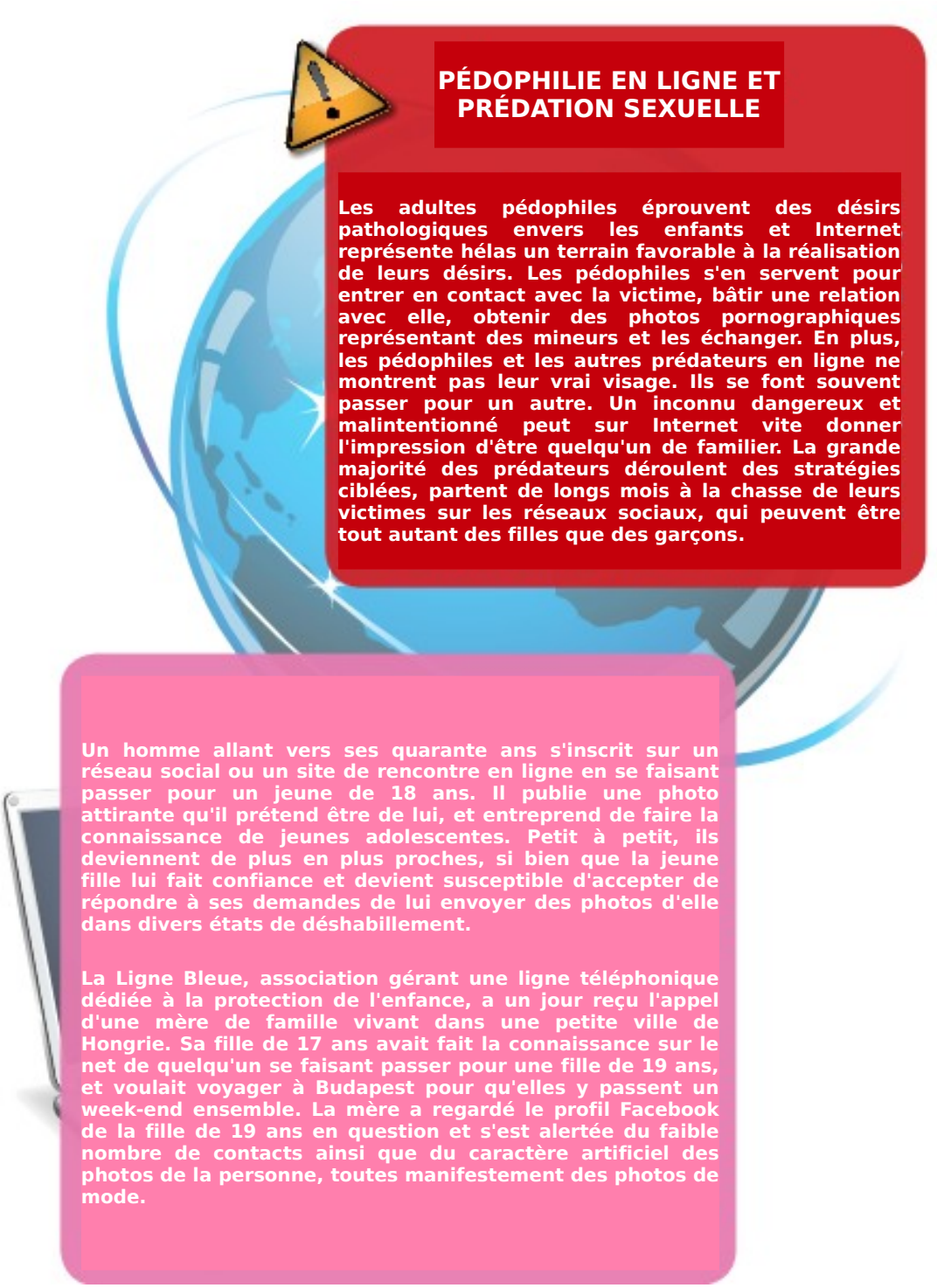
Chat, ou encore clavardage. C'est ce qu'on dit quand deux personnes ou plus dialoguent en temps réel à travers un canal (en anglais chatroom) auquel ils ont accès via un programme spécialement dédié.

Cloud computing

En français, on dit aussi « infonuagique ». L'informatique dans les nuages, c'est tous ces services qui permettent de faire des choses sur un ordinateur en passant par un navigateur web ou une application, sans stocker les données et les fichiers sur son propre ordinateur. Les données sont stockées sur un serveur qui peut être situé n'importe où dans le monde. Les exemples les plus courant sont les webmails (comme Gmail) et les espaces de stockage en ligne (comme Dropbox). Ce type de services est avantageux pour le consommateur, car personnalisés et riches en fonctionnalités. Mais ils posent de véritables inquiétudes pour la protection de la vie privée : il est en effet impossible de suivre la trace de ses données sur le cloud.

Cookie

Ce mot qui veut dire en anglais « biscuit » désigne de courts fichiers qui sont déposés sur l'ordinateur de l'internaute, en théorie avec son autorisation, au cours de sa visite d'une page web. Le but d'un cookie est de simplifier et de rendre plus confortable l'utilisation d'un service web. Il en existe nombreuses variétés, répertoriables en deux grandes catégories : les cookies temporaires, à durée de vie limitée (par exemple les cookies qui permettent l'authentification sécurisée à un service bancaire en ligne), et les cookies permanents (qui peuvent par exemple contenir les paramètres de langue d'un site web). Ces derniers restent sur l'ordinateur de l'internaute tant qu'il ne les supprime pas.



PÉDOPHILIE EN LIGNE ET PRÉDATION SEXUELLE

Les adultes pédophiles éprouvent des désirs pathologiques envers les enfants et Internet représente hélas un terrain favorable à la réalisation de leurs désirs. Les pédophiles s'en servent pour entrer en contact avec la victime, bâtir une relation avec elle, obtenir des photos pornographiques représentant des mineurs et les échanger. En plus, les pédophiles et les autres prédateurs en ligne ne montrent pas leur vrai visage. Ils se font souvent passer pour un autre. Un inconnu dangereux et malintentionné peut sur Internet vite donner l'impression d'être quelqu'un de familier. La grande majorité des prédateurs déroulent des stratégies ciblées, partent de longs mois à la chasse de leurs victimes sur les réseaux sociaux, qui peuvent être tout autant des filles que des garçons.

Un homme allant vers ses quarante ans s'inscrit sur un réseau social ou un site de rencontre en ligne en se faisant passer pour un jeune de 18 ans. Il publie une photo attirante qu'il prétend être de lui, et entreprend de faire la connaissance de jeunes adolescentes. Petit à petit, ils deviennent de plus en plus proches, si bien que la jeune fille lui fait confiance et devient susceptible d'accepter de répondre à ses demandes de lui envoyer des photos d'elle dans divers états de déshabillement.

La Ligne Bleue, association gérant une ligne téléphonique dédiée à la protection de l'enfance, a un jour reçu l'appel d'une mère de famille vivant dans une petite ville de Hongrie. Sa fille de 17 ans avait fait la connaissance sur le net de quelqu'un se faisant passer pour une fille de 19 ans, et voulait voyager à Budapest pour qu'elles y passent un week-end ensemble. La mère a regardé le profil Facebook de la fille de 19 ans en question et s'est alertée du faible nombre de contacts ainsi que du caractère artificiel des photos de la personne, toutes manifestement des photos de mode.

Mon journal de bord de la vie privée : que s'est-il passé avec mes données en ligne cette semaine, ces dernières semaines ou ce mois-ci ?

Avec qui ai-je partagé mes données personnelles ? Qu'est-ce que des proches ou des inconnus ont écrit ou dit à mon sujet ? Ai-je donné mon nom, mon numéro de téléphone ou mon adresse mail à quelqu'un ? Me suis-je inscrit sur un site web ? Est-ce que j'ai téléchargé ou mis en ligne un fichier ? Est-ce que j'ai utilisé une application connectée sur mon téléphone portable ? Etc…

QUIZ

1. Tu rencontres un gars / une fille sur Internet, qui te plaît beaucoup. Vous tchattez depuis longtemps, et quand il / elle te demande de lui envoyer une photo de toi :

a) Enfin ! Mon profil rend tellement bien ! On pourrait peut-être même se rencontrer.
b) Pourquoi pas. Au pire je lui plairai pas.
c) Pourquoi est-ce que je lui en enverrais ? Après tout il/elle n'a qu'à se contenter des photos qu'il/elle voit sur mon profil !

2. Une personne que tu n'as jamais rencontrée te demande en ami sur Facebook. Quelle est ta réaction ?

a) J'accepte, pour avoir le plus d'amis possible sur Facebook
b) Je réfléchis encore pour essayer de me rappeler d'où est-ce que je le connais
c) Je ne réponds pas. Après tout, je ne l'ai jamais vu, et je ne comprends même pas pourquoi il m'a ajouté

3. Tu vois le titre suivant dans un journal : « Mèmes : la dernière mode sur Internet »

a) C'est quoi ça ?
b) Ils en ont vaguement parlé à l'école, il s'agirait d'images gênantes
c) Tu penses à ces fichiers, généralement des images ou des vidéos, qui sont diffusés sur Internet dans un but de divertissement et qui représentent des situations gênantes ou manipulées

4. Tu as 15 ans. Tu voudrais consulter une page web dont l'accès est précédé par le choix entre : « J'ai 18 ans ou plus, j'accède à la page » ou « je n'ai pas encore 18 ans, je quitte la page ».

a) Je ne comprends pas le sens de cette différenciation
b) J'ai beau n'avoir que 15 ans, ça ne m'empêche pas de décider par moi-même ce que je peux voir sur le Net et ce que je préfère laisser de côté
c) Peut-être que je m'épargne une expérience désagréable si je laisse cette page tranquille

5. L'inscription à un jeu vidéo en ligne nécessite l'indication d'un compte bancaire

a) De mon point de vue l'essentiel est de pouvoir enfin jouer à ce jeu
b) Je ne sais pas. Il vaut peut-être mieux demander l'avis de quelqu'un qui comprend mieux que moi ces affaires-là
c) C'est absolument exclu, parce que cela veut dire que je suis dirigé vers un service payant

6. Tu remarques sur un réseau social, que ton amie a mis en ligne des photos de toi en bikini. Quelle est ta réaction ?

a) Je dois saisir l'occasion de mettre moi-même en ligne quelques photos de moi en tenue de plage
b) Peut-être quand même pas des photos en bikini, mais je mettrais bien quelques photos bien réussies de moi
c) Plein de gens vont télécharger la photo sur leur propre ordinateur. Je ne veux pas qu'on puisse me

retrouver sur l'ordinateur d'un autre.

7. Tu reçois un mail qui te dit que tu es l'heureux gagnant d'un voyage de vacances vers une destination exotique. Il te suffit de renseigner ton nom, adresse, numéro de téléphone, compte bancaire, numéro de carte d'identité et ton identifiant fiscal.

a) Quelle veine ! Je remplis ces quelques informations et je pars bientôt en vacances !
b) Comment est-ce que j'aurais pu gagner un tel voyage ? Mais on sait jamais : au cas où, je remplis quand même ce formulaire
c) Mais bien sûr ! Ce sont des escrocs, je ne leur envoie aucune donnée !

8. Ton ami te raconte que quelqu'un envoie des mails en se faisant passer pour lui

a) Mais oui bien sûr ! Comment est-ce que quelqu'un pourrait utiliser son compte mail à sa place ?
b) Il a dû donner son mot de passe à quelqu'un qui lui fait une blague
c) Hélas il n'est de nos jours pas bien difficile de pirater le compte de quelqu'un

9. Tu as entendu à l'école, qu'une photo est une donnée personnelle :

a) Non. Une donnée personnelle, c'est juste le nom, l'adresse, le numéro de carte d'identité, etc… Tout le monde sait ça !
b) Non, sauf si le nom de la personne est écrit dessus
c) Évidemment, car est assez simple d'identifier personnellement un individu sur la base d'une photographie de lui

10. Un de tes proches a été victime d'un abus de données personnelles. Il t'a raconté qu'il s'est adressé à la NAIH pour de l'aide :

a) De toutes façons je comprends pas de quoi il parle
b) Ah… c'est probablement une organisation internationale qui s'occupe de données informatiques
c) Si je ne me trompe pas, il s'agit de l'autorité hongroise de protection des données personnelles

11. On te demande ton numéro de téléphone dans une boîte de nuit

a) Je le donne. J'aime bien faire des rencontres.
b) Pourquoi pas. Au pire je réponds pas.
c) J'ai déjà entendu parler de plusieurs affaires de harcèlement, alors vaut mieux pas

12. Ta sœur de 14 ans ne peut aller sur Internet que sous la surveillance de ses parents

a) C'est quand même gênant qu'elle ne puisse pas faire ce qu'elle veut sur Internet
b) À quoi ça sert d'être assis à côté d'elle ? De toutes façons c'est possible de vérifier son historique.
c) C'est sûrement pas une situation confortable pour elle, mais au moins elle ne voit rien qui ne lui soit pas adapté

13. Un copain a mis en ligne une photo gênante de toi sur Internet

a) Je me fâche un peu mais c'est pas grave. Je lui demande de supprimer la photo et j'oublie l'affaire.
b) Moi aussi je mets en ligne une photo gênante de lui.
c) Il ne manquait plus que ça ! On ne pourra plus jamais supprimer cette photo d'Internet.

14. Je me suis inscrit sur Facebook pour :

a) Que je puisse rencontre le plus de personnes possibles, que je puisse mettre en ligne des photos de moi, partager des vidéos, dire où je suis et qu'est-ce que je fais
b) Ne pas être en reste. Tout le monde est sur Facebook, aujourd'hui, et y collectionne les amis
c) Y chercher mes amis, notamment ceux que j'ai perdu de vue

15. Si on me demande si je fais attention à mes données personnelles, je peux répondre que oui, parce que :

a) Je ne transmets mes données personnelles qu'à des personnes qui me sont sympathiques
b) Je ne donne accès à mes données personnelles que si on me le demande, je ne le fais pas de ma propre initiative
c) Je n'ai pas l'habitude de partager mes données personnelles sans raison avec n'importe qui

RÉSULTATS

Si tu as choisi une majorité de A

Les réponses que tu as données nous font conclure que tu devrais faire plus attention à la protection de tes données à caractère personnel. Tu ne mesures pas bien les conséquences de certaines de tes actions, par exemple lorsque tu donnes sans y réfléchir, à n'importe qui, ton numéro de téléphone, ou que tu mets en ligne des photos de toi sur les réseaux sociaux. Nous te conseillons de lire notre livret sur la protection de données, qui contient des informations utiles pour mieux te protéger !

Si tu as choisi une majorité de B

Il ressort de tes réponses que tu as déjà entendu parler de la protection des données personnelles. Tu comprends le sujet intuitivement. Tu sais te montrer méfiant lorsque la situation l'exige, et qu'on te demande certaines informations personnelles. Mais tu finis quand même en général par dévoiler un grand nombre de celles-ci. La lecture de notre livret sur la protection des données à caractère personnel peut t'aider à parfaire tes connaissances et à mieux te protéger.

Si tu as choisi une majorité de C

Félicitations ! Tu as réussi haut la main le quiz de la protection des données personnelles ! On voit à partir de tes réponses que tu maîtrises les questions sur la protection de tes données. Tu sais faire la part des choses dans ta vie quotidienne, et déterminer en toute conscience quand est-ce qu'il est nécessaire de divulguer des données personnelles, ou quand est-ce qu'une trop grande diffusion peut s'avérer dangereuse. Continue comme ça, et n'hésite pas à approfondir tes connaissances en lisant notre livret !

CONSEILS POUR BIEN NAVIGUER SUR INTERNET

Conseils généraux

- Ton style te détermine. Ne te fais pas insulte à employer des propos vulgaires.
- Utilise des mots de passe complexes et change les régulièrement.
- Au lieu de les ouvrir, supprime les messages en provenance d'adresses suspectes. Ne clique pas n'importe où sans réfléchir.

Réseaux sociaux

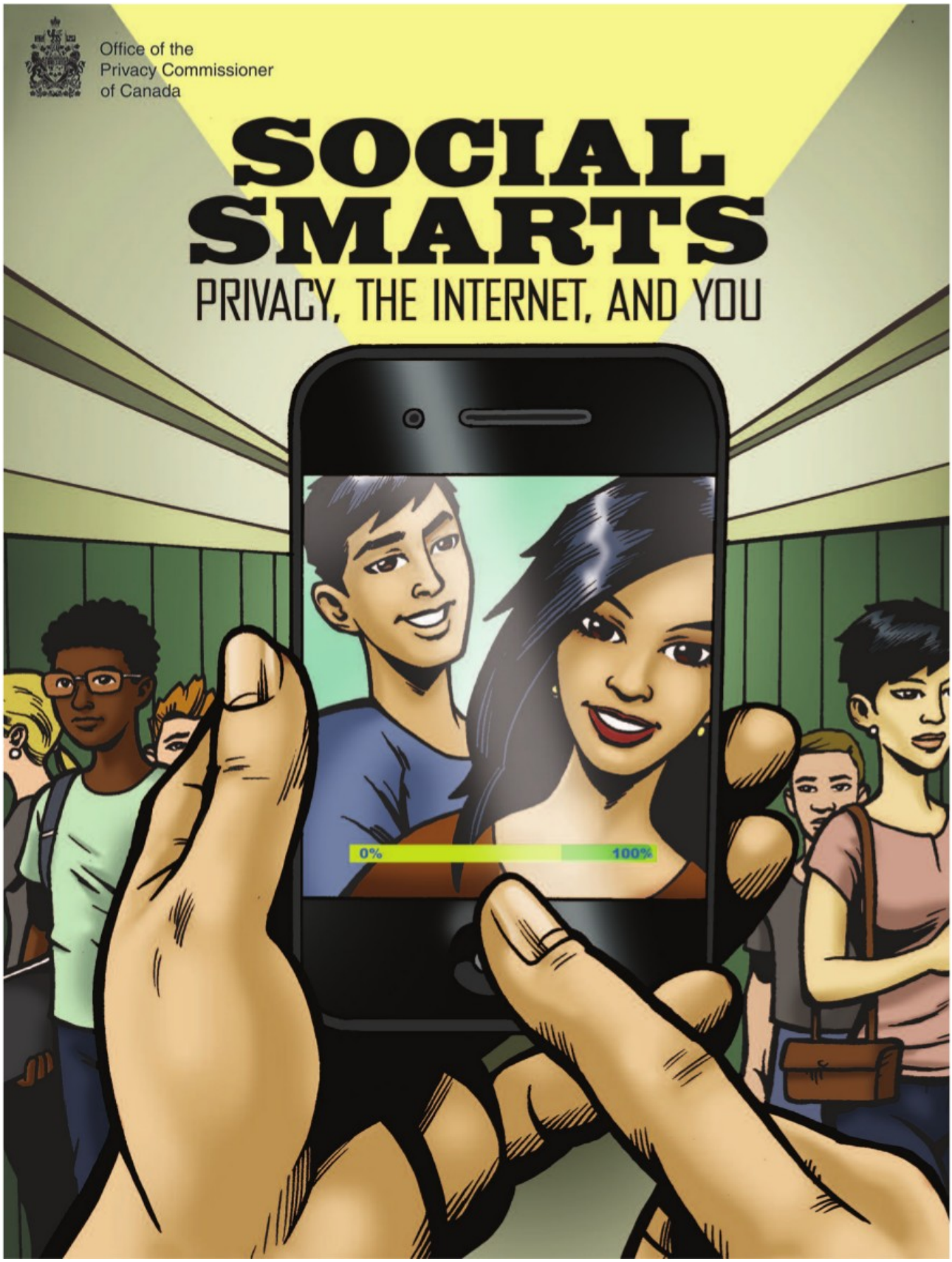
- Prends connaissance des paramètres de sécurité et de confidentialité et utilise les !
- Avant de poster un message, réfléchis bien aux informations sur toi qui seront ainsi mises en ligne.
- Ta réputation en ligne est d'une grande valeur, prends-en soin.
- Les informations vraiment personnelles, privées, ne doivent pas devenir publiques.
- Il vaut mieux avoir un nombre faible mais fiable d'amis.
- Le chemin qui mène droit est toujours le plus court : sois honnête avec tes amis, parlez ensemble de ce qui peut vous blesser pour éviter les malentendus.
- Si quelqu'un te menace ou te harcèle sur Internet, il faut immédiatement prévenir les administrateurs et les adultes autour de toi, imprimer ou sauvegarder une preuve, puis bloquer la personne menaçante.

Les terminaux mobiles

- N'oublie pas que sur Internet, tu n'es jamais seul !
- Sois conscient du fait que si on te vole ton appareil, par exemple ton portable, on te vole aussi les données personnelles qu'il contient.
- Utilise aussi un mot de passe sur ton téléphone, ainsi que les autres mesures de sécurité qui y sont disponibles.
- Si tu veux acheter une application, pense avant à vérifier les informations auxquelles elle exige l'accès, comme par exemple les données de géolocalisation.
- Tu peux activer et désactiver la géolocalisation.
- Les réseaux publics, comme les hotspots wifi, ne sont pas sûrs, et peuvent représenter un danger pour tes données personnelles.
- En cas d'achat en ligne, pense à vérifier sur ton relevé bancaire les montants prélevés.
- Supprime et bloque les appels et messages suspects que tu reçois
- Demande toujours l'autorisation des gens que tu filmes ou prends en photo
- Ne diffuse pas les photos ou les vidéos d'autres personnes que toi sans leur autorisation

ET LE PLUS IMPORTANT……

Ne fais pas aux autres, ce que tu ne voudrais pas que l'on fasse avec toi. S'il t'arrive des ennuis, tu n'es sûrement pas le seul à faire face à une telle situation, alors demande tout de suite de l'aide aux adultes autour de toi !



Cette bande dessinée, réalisée par le Commissariat à la protection de la vie privée du Canada, a été traduite en hongrois dans le cadre de notre projet.
Une version française est à l'adresse : www.priv.gc.ca/youth-jeunes/fs-fi/res/gn_index_f.asp

Autorité Nationale pour
la Protection des Données
et la Liberté de l'Information

Autorité Nationale pour la Protection des Données et la Liberté de l'Information
(NAIH)

1125 Budapest, Szilágyi Erzsébet fasor 22/C
Adresse postale : 1530 Budapest, Pf.: 5

Tél : +36 (1) 391-1400
Fax : +36 (1) 391-1410
Internet : http://www.naih.hu
Courriel : ugyfelszolgalat@naih.hu , privacy@naih.hu