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

LA CLEF DU CYBERESPACE

Etude de la NAIH pour un usage sûr et conscient d'Internet par les enfants
Extrait traduit en français
2nde édition
2016

La clef du cyberespace

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

(extrait)

(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)

2016

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

Krisztina Mária Bácskai

Nóra Belső

Dániel Eszteri

Laura Kozma

Ágnes Lux

Petra Márkus

Attila Mátyásfalvi

Sára Ránki

Borbála Csekeő Reményiné

Bence Ságvári

Gabriella Sárközi

Dániel Somfalvi

Katalin Somogyvári

Júlia Sziklay

Zsófia Tordai

Direction de l'étude:

Júlia Sziklay

Traduction:

Julien Rossi

Version intégrale disponible en hongrois et en anglais sur www.naih.hu

Deuxième édition, 2016. ISBN 978-963-08-7155-6

Autorité nationale de protection des données et de liberté de l'information

Table des matières

1. PRÉSENTATION DE L'AUTORITÉ NATIONALE DE PROTECTION DES DONNÉES ET DE LA LIBERTÉ DE L'INFORMATION

L'Autorité Nationale de Protection des Données et de 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 32 255 euros (montant en vigueur en septembre 2016).

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.

C'est ainsi qu'en 2015, parallèlement à la présente étude, des supports pédagogiques réalisés dans le cadre d'un projet international ont été publiés à l'attention des enseignants et des éducateurs. Intitulés, en hongrois, *Európai Kézikönyv a Magánszféra- és a Személyes Adatok Védelemről Iskolák Számára* ainsi que *Adatvédelmi Kézikönyv Pedagógusoknak,* ils sont librement téléchargeables sur notre site Internet www.naih.hu .

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

2. PRÉFACE

> « 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 des fardeaux et misères de l'existence sociale. »
>
> – 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 lesquels 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,

---

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*

campagnes d'information et organismes s'y intéressent, y compris en Hongrie. Il ne faut cependant pas perdre de vue les nombreux avantages et effets bénéfiques pour les enfants du « Réseau des Réseaux ». Dans les rédactions à l'épreuve de hongrois du concours d'entrée au collège de 2013, les élèves de quatorze ans ont écrit par exemple :

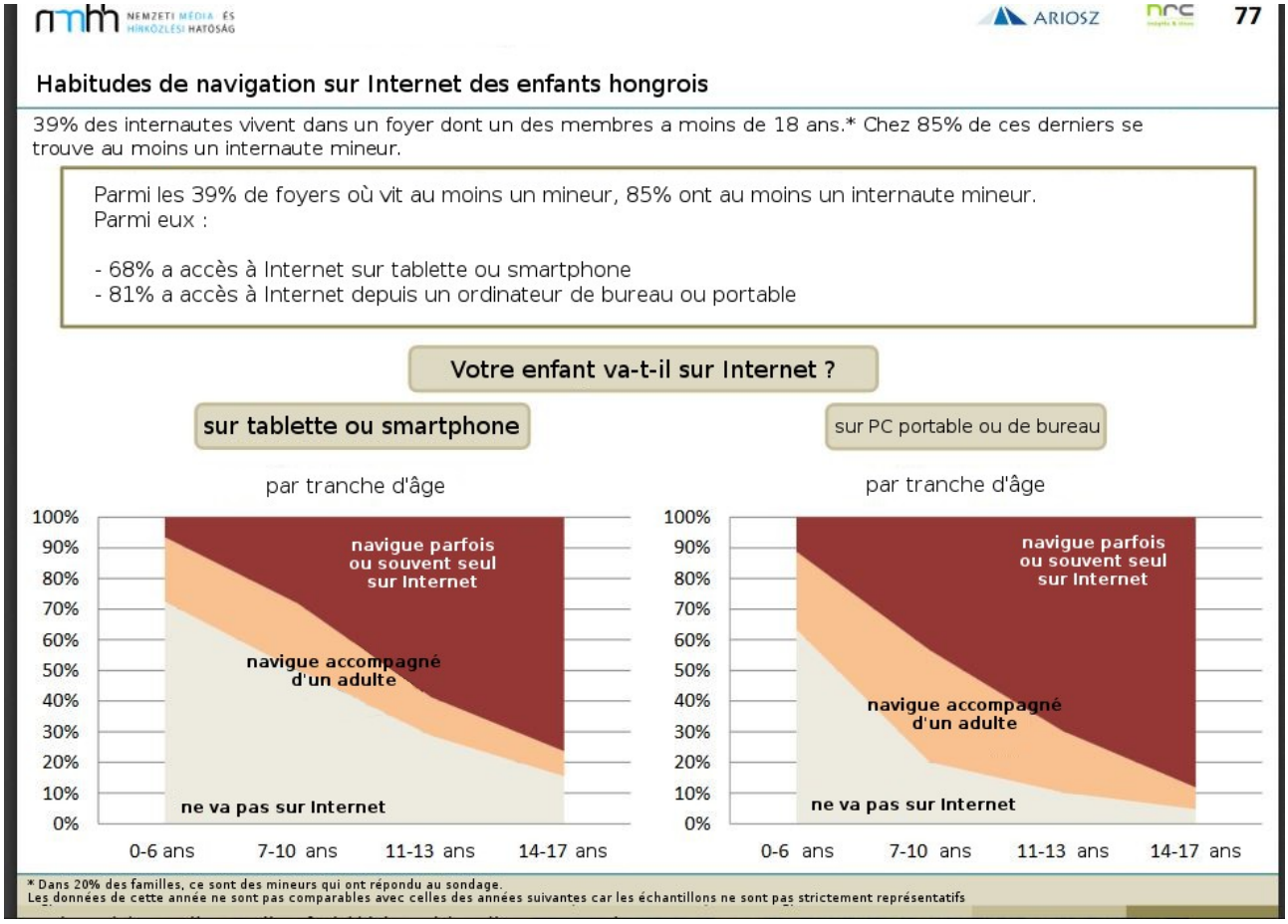
> « Internet est très important et utile pour l'humanité, car aujourd'hui on peut tout y trouver. Grâce à lui, nous pouvons très facilement parvenir à des informations ou à des documents importants. La majorité des gens – et surtout les adolescents – passe par contre plus de temps à naviguer sur les réseaux sociaux qu'à apprendre sur Internet »
>
> Ou encore :
>
> « On trouve beaucoup plus facilement des informations et on garde beaucoup mieux le contact avec ceux qui vivent loin en allant sur Internet, mais on y lit probablement beaucoup plus d'informations superflues qu'utiles »

Si depuis 2010, Internet est devenu la principale source d'information pour les jeunes Américains[9], cette proportion est de 48 % chez les Hongrois de 14 à 19 ans[10]. Il n'y a plus ni barrière de temps ni d'espace. Les frais de duplication, sont, parmi d'autres, abolis. Le stockage et la recherche d'information de toutes les qualités et sous n'importe quel format devient un véritable « jeu d'enfant ». La toile mondiale peut offrir un terrain parfaitement propice aux loisirs constructifs, au développement des aptitudes de l'enfant et à la formation d'amitiés, lorsque son usage se déroule dans un cadre éduqué et protégé.

société de l'information entre 1995 et 2009, et qui sont aujourd'hui généralement à l'âge de l'adolescence.

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

10 Selon une enquête en ligne de marché commandée par l'Autorité Nationale des Médias et des Communications (NMHH) en 2014 sur les habitudes de consommation de la population sur Internet : http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf . Page consultée le 12 février 2016.



Une étude comparative hongroise de 2010 sur les habitudes des enfants de 10 à 18 ans[11] concluait que leurs principales motivations à utiliser Internet étaient (respectivement chez les garçons et les filles) : le maintien de contact sur les réseaux sociaux (47 % et 53%), le divertissement (46 % et 37%), le jeu (29 % et 6 %) et, enfin, l'apprentissage (5 % et 4%). Ceci étant dit, cet ordre était différent chez ceux qui se connectaient au moins une fois par semaine. Leurs objectifs étaient cette fois plutôt l'apprentissage (40 % chez les garçons et 50 % chez les filles), le divertissement (37 % et 45%), les activités communautaires comme les réseaux sociaux (32 % et 35%) et le jeu (43 % et 26%).

Presque tout le monde utilise des moteurs de recherche en lien avec une activité d'apprentissage, l'usage de dictionnaires électroniques s'est répandu tout autant que la consultation de Wikipedia s'est généralisée. Même si cela est plus rare, certains consultent également des collections thématiques de liens, les sites web proposant du matériel pédagogique ou centralisant des essais, ou encore des pages proposant des tests de langue ou des examens blancs.

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

11 SZÉKELY, Levente. 2010. „Internetcsizma az iskolapadon" in *Új Ifjúsági Szemle*, hiver, pp. 79-87

évolution, et sur le fait qu'il s'agit de ne pas y accoler de jugement de valeur. Ceci étant dit, il demeure recommandable d'adopter une posture critique, prudente et consciente permettant l'analyse des phénomènes de fond dans ce domaine.

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. 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.

Pour que les enfants soient préparés et formés à utiliser de façon informée les outils modernes d'information et de communication sans être les proies du monde numérique, il est de ma conviction que la formation des acteurs du monde de l'enseignement et de l'éducation aux aspects théoriques et pratiques de la protection des données est devenue indispensable. C'est pour cela que j'ai demandé en mars 2016 au ministre en charge de l'instruction publique et aux instituts de formation des enseignants d'introduire une formation à la protection des données dans le cursus des futurs enseignants. La NAIH sera heureuse de prêter tout son concours à une telle initiative, en mettant à disposition son expérience, ses productions intellectuelles ainsi que son réseau à l'international.

Le succès de l'édition 2013 de notre ouvrage *La clef du cyberespace* montre que le besoin de partage d'expérience et de bonnes pratiques parmi les professionnels de l'enseignement, de l'éducation et de la protection de l'enfance est grand. C'est ce qui a motivé en 2016 la publication d'une édition augmentée et mise à jour de cette étude, qui n'aurait été possible sans le soutien de l'Autorité Nationale des Médias et des Communications, que je profite de ces pages pour remercier.

Dr. Attila Péterfalvi
Président de l'Autorité de la protection des données et de la liberté de l'information

3. PRÉSENTATION DE QUELQUES CAS ÉTUDIÉS

A. La pratique de l'autorité hongroise de protection des données à caractère personnel

Que ce soit auprès du Commissaire à la protection des données ou auprès de l'Autorité nationale de la protection des données et de la liberté de l'information (NAIH), qui a succédé à cette première en 2012, de nombreuses plaintes ont été déposées en rapport avec des infractions commises en ligne.

En tant qu'autorité indépendante de protection des données personnelles, la NAIH 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.

Voici quelques exemples de cas ayant été traités par le Commissaire à la protection des données (ABI)[12] :

- L'ami d'un requérant avait utilisé une photo de lui, mise en ligne sur le réseau social iWiW, pour une couverture de livre ésotérique, à son insu et contre son gré. Dans la mesure où la personne concernée n'avait rien à voir avec le thème du livre, et qu'elle ne souhaitait pas volontiers donner son visage à un tel livre peu avant la défense d'un titre universitaire, la publication était bel et bien de nature à lui porter préjudice (2534/P/2009)
- Une mère s'est tournée vers le commissaire à la protection des données car une photo de son enfant accompagnée d'une légende au texte dégradant avait été mise en ligne sur Facebook. Dans la mesure où Facebook ne dispose pas d'un établissement ni de serveurs en Hongrie, mais d'un centre en Irlande, cette entreprise est soumise au droit de l'Union en matière de protection des données, lequel forme le socle du droit hongrois en la matière. La mise en ligne de la photo de la personne mineure concernée sans son autorisation et celle de ses représentants légaux constitue donc une infraction. Le commissaire à la protection des données a informé la mère de la possibilité d'exiger de Facebook le retrait du contenu injurieux et de la possibilité de déposer plainte au civil, ou, selon les circonstances, au pénal (ABI-7949/2012/P)
- 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

12 *NDT* : une partie des cas décrits dans la version intégrale seulement ont été sélectionnés ici pour traduction

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)
- Dans une autre affaire, des photos de la fille âgée de 16 ans du requérant avaient été copiées de www.my-vip.com sur www.pedomaci.hu avec son nom complet, son adresse, son âge et son numéro de téléphone. Elle reçut des lettres de menace et fut harcelée au téléphone. Des commentaires injurieux furent associés à sa photo. Les opérateurs du site avaient répondu aux demandes de suppression que « tu ne disparaîtras plus jamais de ta putain de vie de [ce site] » (ABI-4865/2012/P)

En raison de la récurrence de plaintes visant un même groupe de sites web, le commissaire à la protection des données déposa plainte contre X le 15 février 2011 pour infraction au droit à la protection des données à caractère personnel. Les sites en cause étaient : www.tundermacko.info, www.pedomaci.net, www.puruttya.hu, www.sunaszemle.hu, www.agyiszint.hu et www.napiszar.hu. Les compagnies ayant fourni le service d'hébergement de ces sites Internet n'ont pas été capables de nommer les responsables des noms de domaine en cause, ce qui a nécessité l'ouverture d'une enquête. Malheureusement, la capitainerie de police du XIIIe arrondissement de Budapest a refermé l'enquête le 28 juillet 2011. Depuis, l'enquête a été rouverte sur ordre du procureur des Ve et XIIIe arrondissements de Budapest.

La nouvelle loi hongroise de protection des données à caractère personnel dote la NAIH, qui a pris la place de l'institution du Commissaire à la protection des données, d'un nouvel outil : la procédure administrative de sanction. Elle a eu plusieurs fois l'occasion de la mettre en œuvre, aux côtés de la procédure plus classique de médiation :

- 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 (NAIH-5951/2012-H)
- La publication dans des journaux, qui peuvent être des journaux en ligne ou des portails d'information, de données personnelles comme le nom, la date de naissance et le nom de la mère dans les rubriques des naissances comporte des risques en matière de protection des données (NAIH/2015/503/V)
- La NAIH a été contactée dans une affaire concernant les concours de beauté pour enfants. Des requérants se sont plaints de ne pas pouvoir identifier le responsable de traitement de sites Internet d'agences de manequinat, ni ses coordonnées, ni même la moindre politique de confidentialité. L'affaire était encore en cours lors de la rédaction de la présente étude (NAIH/2016/330/V)

B. La pratique du 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. Il gère ainsi depuis 2008 un site dédié aux droits des enfants (www.gyermekjogok.ajbh.hu) et une page Facebook depuis 2011 (www.facebook.com/Gyermekjogok). Il arrive rarement au Médiateur de traiter des demandes relatives à la protection de l'enfance sur Internet, puisque dans la mesure où elles impliquent généralement une infraction au droit à la protection des données, elles ne sont pas dans son champ de compétence. Cela ne l'empêche pas de pouvoir lancer des projets en rapport avec les droits des enfants. Ainsi, en 2015, le Médiateur s'est intéressé à l'évaluation de l'éducation aux médias en Hongrie.

La recommandation de la Commission européenne de 2009 relative à l'éducation aux médias[13] encourage l'intégration aux programmes d'enseignement d'une éducation critique à la lecture des médias. Selon les professionnels de l'éducation et de l'enseignement, les enfants ont cependant un accès inégal à ce type d'enseignement en fonction des possibilités locales, personnelles et scolaires qui leur sont offertes.

L'éducation aux médias est apparue pour la première fois en 2013 dans le Programme national d'enseignement fondamental (*Nemzeti Alaptanterv*, NAT), comme rubrique dans la matière intitulée « culture visuelle ». Cependant, l'enquête du Médiateur a montré que seule l'étude des programmes locaux pouvait donner une image des pratiques réelles d'éducation des enfants à la lecture critique des médias. Ainsi, le conseil des enseignants peut décider d'intégrer de faire de cette formation une matière à part entière, ou bien de l'intégrer à une autre, comme la littérature, l'informatique, parfois le dessin ou la culture visuelle. Lorsqu'elle est intégrée à une autre matière, le nombre d'heures d'enseignement de celle-ci est augmentée du nombre d'heures que le programme national attribue à l'éducation aux médias. Mais, dans la pratique, ces heures complémentaires ne sont pas toujours utilisées aux fins prévues.

Dans le système éducatif hongrois, les compétences requises pour l'enseignement de l'éducation aux médias peuvent s'acquérir au cours d'une licence en culture audiovisuelle et médiatique, d'un Master en enseignement de la culture audiovisuelle et médiatique, ou dans une formation intégrée de cinq ans de professeur de média, audiovisuel et communication. Mais seuls 20 % à 30 % des enseignants de culture médiatique disposent de la formation professionnelle adéquate, ce qui peut en partie s'expliquer par l'absence de normes obligatoires de formation. Dans la pratique, l'éducation aux médias revient aux enseignants que la matière intéresse, ou à qui cette mission est confiée, indépendamment de son degré de compétence.

Le faible nombre d'heures dédiées, l'intégration de cet enseignement à d'autres matières, et le faible nombre d'enseignants adéquatement formés sont autant de facteurs qui, dans de nombreux cas, font obstacle à une éducation critique aux médias efficace et de qualité.

Ces éléments posent d'autant plus problème que, selon les conclusions du Médiateur, les

13 Recommandation 2009/625/CE de la Commission du 20 août 2009 sur l'éducation aux médias dans l'environnement numérique pour une industrie de l'audiovisuel et du contenu plus compétitive et une société de la connaissance intégratrice

enfants ne sont souvent pas conscients des dangers de l'usage des médias sociaux, que tout le monde est loin de connaître les paramètres de confidentialité, et qu'en cas de harcèlement, peu savent vers qui se tourner.

Le comité hongrois pour l'UNICEF évoque dans son programme intitulé *Réveil* (*Ébresztő-óra*) et destiné aux écoliers la question de la sécurité en ligne. Selon un sondage réalisé en 2014 par cet organisme, un tiers des enfants hongrois a été victime d'insultes sur Internet. 53 % de ces victimes avait tenté de se défendre, 26 % a vite refermé la page, mais seuls 11 % ont demandé de l'aide. 47 % des enfants jugent que l'Internet n'est pas sûr. Dans le même temps, 96 % des enfants de 10 à 18 ans dispose d'un téléphone portable, et 88 % d'un profil sur un réseau social. *Il est à noter que 78 % des 10-12 ans dispose déjà d'un profil, alors qu'officiellement, seuls ceux âgés de 13 ans ou plus auraient dû pouvoir s'inscrire*.

L'analyse de la situation hongroise en matière d'éducation aux médias ne peut bien sûr faire l'impasse sur la situation en matière de litératie numérique, c'est-à-dire en matière de formation aux compétences dans l'usage des outils et technologies numériques. Si ce dernier sujet n'était pas au programme de l'enquête réalisée en 2015 par le Médiateur, il est à noter qu'aujourd'hui, *en Hongrie, les possibilités en matière d'accès aux outils numériques sont extraordinairement variables d'un établissement scolaire à l'autre*. Or, selon le Médiateur, l'accès à une infrastructure numérique permettant partout un accès de qualité à Internet est une condition de base pour l'éducation aux médias numériques.

L'analyse du Médiateur a également permis de montrer que l'éducation aux médias, et aux médias numériques, est intimement liée à la sensibilisation aux droits des enfants et des internautes face à la recrudescence de cas de harcèlement en ligne. Très peu d'enfants sont aujourd'hui armés efficacement contre ce phénomène. Or, ni le programme cadre national, ni les formations des instituteurs et professeurs du secondaire n'intègrent d'exigences à ce sujet.

Ainsi, en conclusion, si le programme national d'enseignement fondamental fixe bien comme objectif cadre l'éducation critique des enfants aux médias, cet objectif est aujourd'hui encore largement dépourvu de contenu et laisse à désirer dans sa réalisation concrète.

C. Exemples de cas portés à la connaissance de la police[14]

Les crimes en-ligne touchant des enfants et portés à la connaissance de la police sont souvent des crimes accessoires ; ils ont été commis dans l'objectif de pouvoir commettre un crime encore plus grave.

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

14 Avec nos remerciements à la Capitainerie nationale de la police, et plus particulièrement au colonel de police dr. Sándor Gömbös, au lieutenant-colonel de police dr. Henrik Szabó ainsi qu'au capitaine de police Zsolt Szabolcsi, pour leur coopération et les informations qu'ils nous ont transmises

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.

Par ailleurs, l'expérience de la police a montré que certains criminels se rendent sur des réseaux sociaux directement à des fins de repérage de leurs futures victimes. Ils feignent de tomber amoureux, promettent un emploi d'hôtesse ou de modèle, promettent l'accès à une école d'Europe de l'Ouest, incitant les enfants à se rapprocher d'eux.

Quant à l'usurpation d'identité, celle-ci peut dans certains cas avoir des effets sur toute la vie de la personne. Cela peut se produire lorsque l'usurpateur crée un faux profil sur un réseau social, y met en ligne des contenus affectant la dignité de la victime, voire injurie d'autres utilisateurs, ou se cache derrière l'identité de sa victime pour commettre toute sorte d'actes criminels. Pour cela, cette personne doit disposer des données personnelles nécessaires à rendre crédible un faux profil, qu'il peut trouver facilement sur un profil réel bien fourni en informations et aux paramètres de confidentialité faibles.

Le fait que les adolescents puissent avoir tendance à rajouter des inconnus dans leur liste de contacts rien que pour prouver qu'ils ont le plus large cercle d'amis est également un sujet de préoccupation. La pratique consistant à recueillir les traces numériques des jeunes pourrait bien être beaucoup plus répandue qu'on ne le pense au premier abord. Comme les réseaux sociaux, les partages et les commentaires font partie de la vie quotidienne des jeunes, si un délinquant est suffisamment patient, il peut se procurer des informations dont sa victime n'aurait pas voulu qu'elles parviennent entre ses mains. Les commentaires postés sur divers forums avec une ancienne adresse de courrier électronique inusitée depuis longtemps, les photos avec des amis dans des lieux de divertissement – que la victime soit ou non « taggée » dans l'image – peuvent se muer en une telle source d'informations pour un prédateur, de même que peuvent l'être dans certaines circonstances des connaissances ou des parents souvent plus âgés bien intentionnés, comme une grand-mère, mais maîtrisant mal la navigation et mettant ainsi en ligne publiquement des contenus privés sur la victime sans le savoir.

Les logiciels de messagerie instantanée sont une autre façon de s'approcher de sa victime. En portant en eux la possibilité de l'anonymat, ils permettent au prédateur de mettre à profit la naïveté et la crédulité des enfants. Ce faisant, ils peuvent extraire d'une conversation avec leurs victimes des données personnelles sur celles-ci, convenir d'un rendez-vous, ou les forcer à s'exposer à du contenu agressif. D'un point de vue légal, il est cependant souvent difficile d'établir un délit d'atteinte à la personne, dans la mesure où l'obtention de données personnelles et notamment d'images de la victime se fait avec l'accord de cette dernière. De plus, la fonction d'historique de conversation n'étant pas toujours activée, il est parfois difficile pour les enquêteurs de retrouver la trace du délit.

Le fait de prendre connaissance du contenu de la correspondance d'autrui est équivalent à un délit de violation du secret de la correspondance. Un cas typique se produit lorsque la victime oublie, dans une école ou un cybercafé, de se déconnecter de son compte ou bien de décocher la case permettant au navigateur de se rappeler de son mot de passe. Les applications en synchronisation permanentes sur le téléphone portable (Facebook, Gmail, Viber etc.) permettent aussi à des personnes non autorisées, comme des camarades de classe ou des amis, de regarder les

profils des uns et des autres, de poster au nom des autres. Il peut être difficile même pour un jeune de se tenir à jour d'un progrès technique permanent et rapide, ce qui le rend encore plus vulnérable dans l'environnement numérique.

D. 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.

La version originale en langue hongroise, ou la version traduite en anglais proposent des panoramas plus exhaustifs que le présent résumé en langue française.

4. DES HABITUDES SUR INTERNET DES ENFANTS HONGROIS[15]

A. Tendances générales

Les études de ces dernières années permis d'observer que les enfants hongrois se rendent de plus en plus tôt de façon autonome sur Internet. Pour la plupart, le passage à l'autonomie a lieu entre 8 et 10 ans. Ce passage dépend à la fois de l'âge et du type de parc informatique disponible à la maison (ordinateur traditionnel, terminaux mobiles...) et de sa taille (nombre de terminaux disponibles). En automne 2015, les élèves de 7e année avaient commencé à naviguer sur Internet en autonomie à l'âge de 8 ans en moyenne, contre 10 ans pour les élèves fréquentant la 11e année au même moment. Le temps quotidien passé sur Internet, y compris en semaine, se mesure pour ces enfants en heures, même si cette durée est très dépendante de l'âge des enfants :

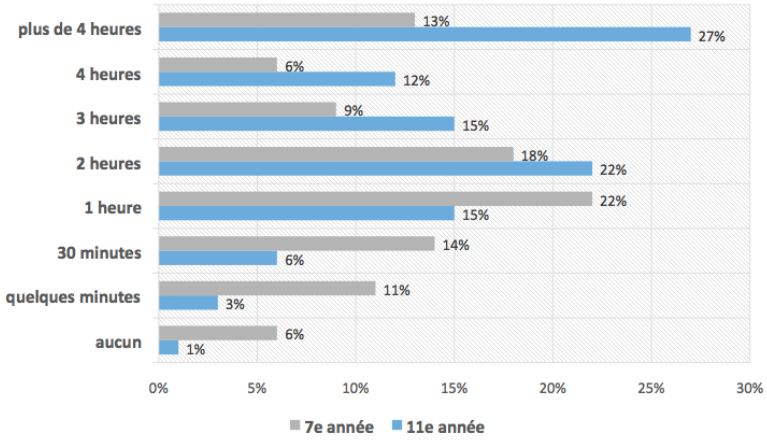


Figure 1 : Temps passé en ligne les jours de classe

Sans surprise, la durée moyenne qu'un enfant hongrois passe sur Internet est encore bien plus forte le week-end qu'en semaine. Ainsi, presque la moitié des enfants de plus de 15 ans passe 4 heures ou plus par jour sur Internet en dehors des jours de classe. Par ailleurs, les données collectées montrent que les filles, et celles et ceux qui disposent de leur propre appareil pour accéder à Internet, y passent plus de temps que la moyenne.

15 L'auteur de ce chapitre est dr. Bence Ságvári. Il est basé sur une étude représentative menée dans les écoles primaires et secondaires hongroises, commandée en 2015 par le Service de Sauvetage des Enfants (*NDT :* International Children's Safety Service en anglais, Nemzetközi Gyermekmentő Szolgálat en hongrois) et réalisée par ITHAKA Nonprofit Kft. 1200 élèves de 7e année et 1200 élèves de 11e année y ont pris part en répondant à un questionnaire dans un contexte scolaire. D'un point de vue statistiquement rigoureux, l'étude porte donc uniquement sur ces deux tranches d'âge bien définies, et non sur les jeunes en général. Tout en tenant compte de ces limites, une approche un plus flexible mais plus opérationnelle nous permet cependant d'en généraliser les conclusions à l'ensemble des jeunes de 13 à 18 ans.

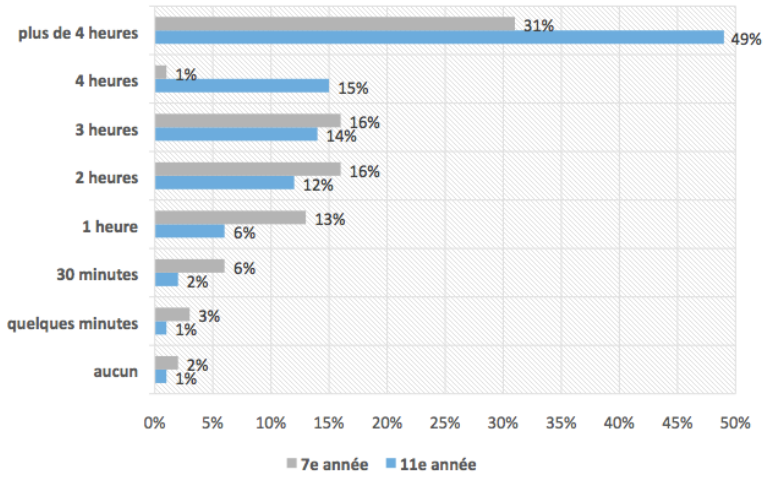


Figure 2 : Temps passé en ligne en dehors des jours de classe

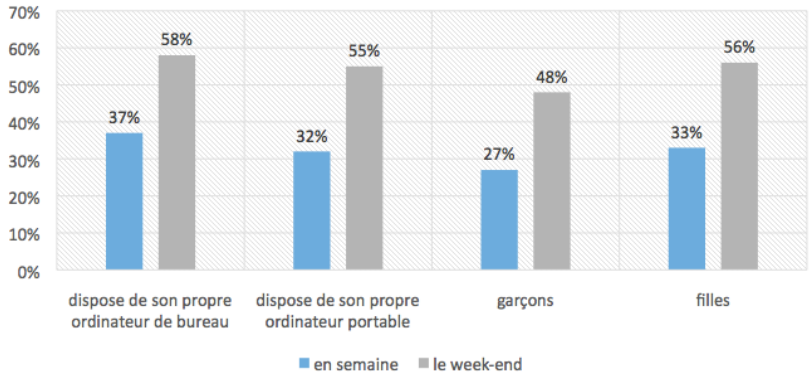


Figure 3 :Proportion passant plus de trois heures par jour sur Internet, en semaine ou le week-end, disposant ou non de son propre équipement d'accès à Internet et selon le sexe de la personnel

La proportion des enfants se rendant souvent sur Internet pendant leurs déplacements a fortement augmenté ces dernières années. Elle atteint désormais 30 % des élèves de 7e année et 61 % des élèves de 11e année. Par ailleurs, le temps passé sur Internet est fortement dépendant du fait de disposer ou non de son propre équipement d'accès. S'il n'y a pas de différence significative de taux de possession d'un téléphone portable intelligent (*smartphone*) entre les élèves de 7e année et ceux de 11e, ceux de 11e année sont cependant plus susceptibles de disposer d'un ordinateur à eux dans leur chambre.

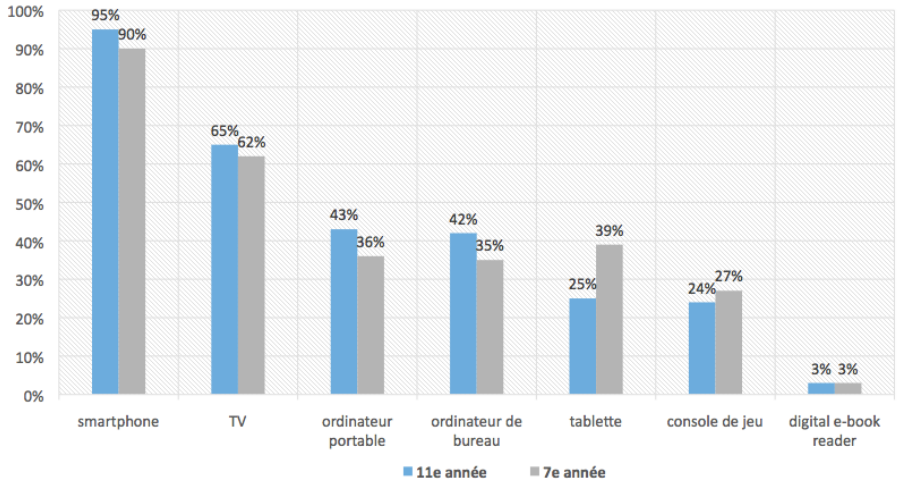
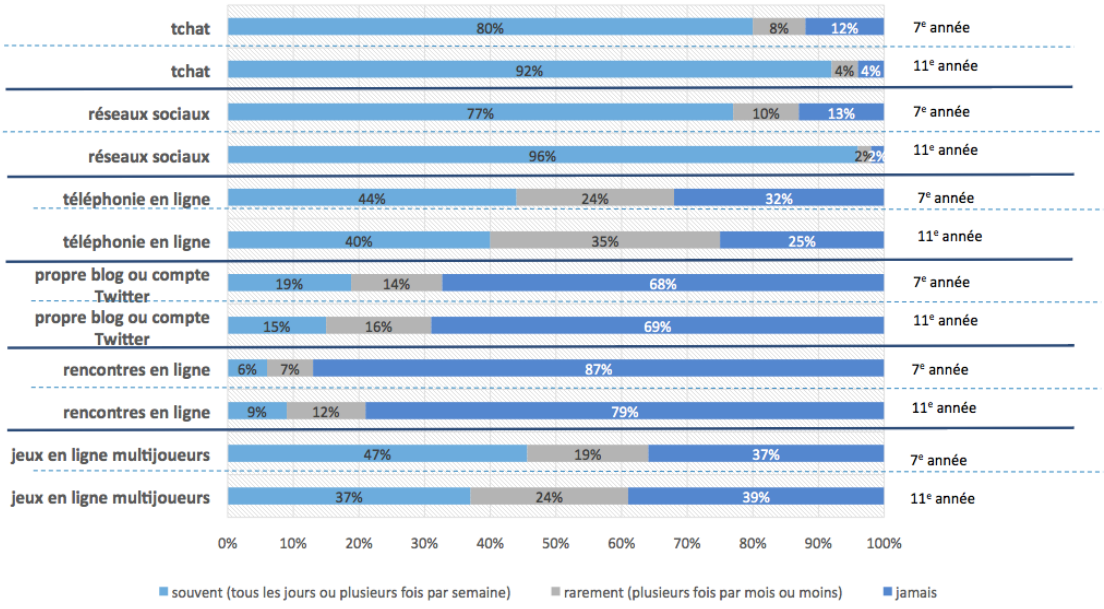


Figure 4 : Enfants en possession de leur propre terminal d'accès à Internet, ou d'un terminal d'accès à Internet dans leur chambre, par type et répartis selon les deux classes d'âge étudiées

Ces quelques dernières années, le téléphone portable est devenu une des plus importantes plate-formes d'accès, ce qui est cohérent avec le fait que l'écoute et le téléchargement de musique soit une des activités les plus populaires sur Internet.



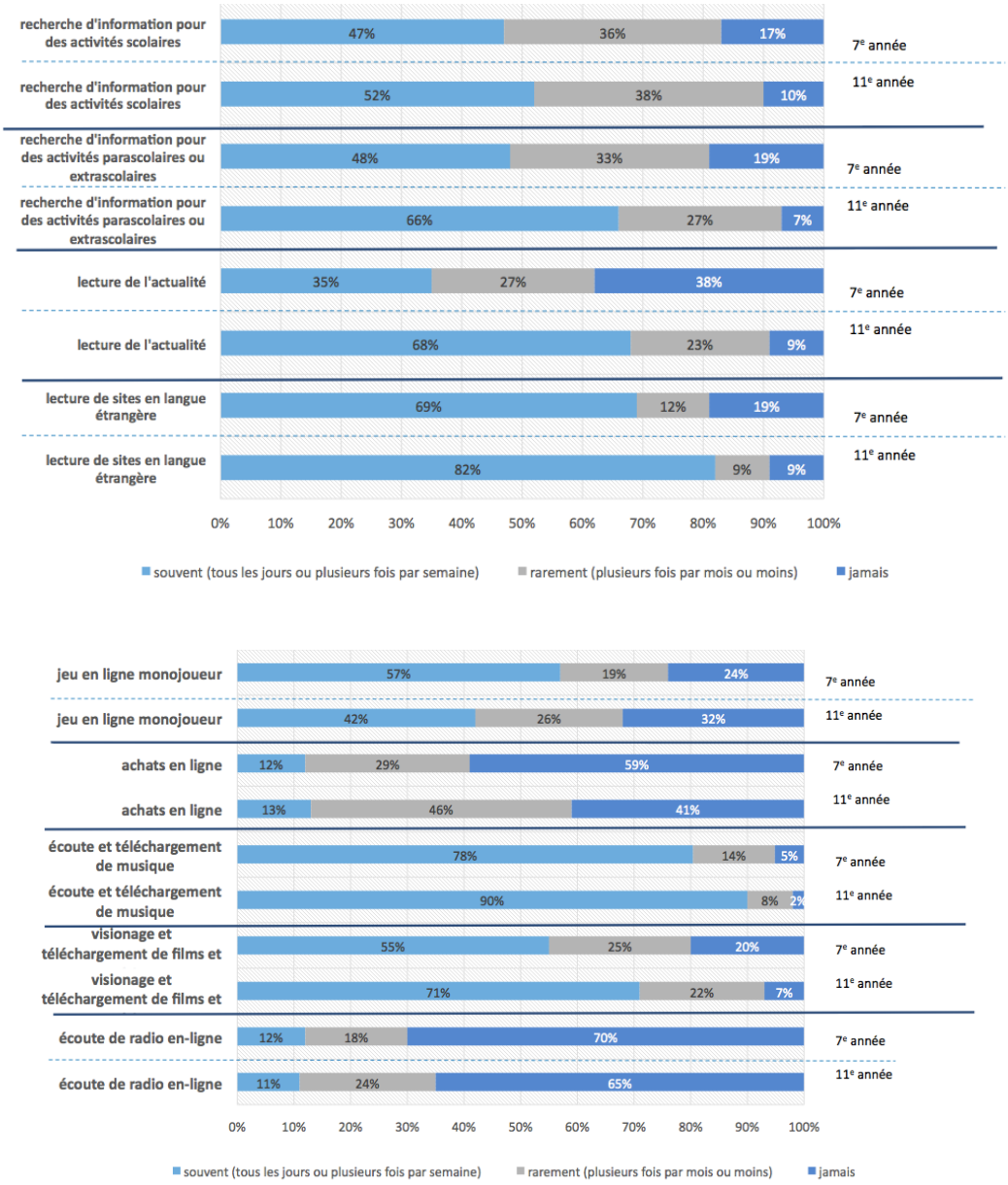


Figure 5 : Popularité des activités en ligne par type d'activité et par tranche d'âge étudiée

B. Réseaux sociaux

Pour une part importante des jeunes, l'utilisation d'Internet est synonyme d'utilisation des réseaux sociaux. Les actualités, informations, contenus sérieux ou divertissants qu'ils consultent ont souvent été partagés avec eux par des amis. Le simple fait d'observer le temps passé par la tranche d'âge étudiée sur les réseaux sociaux suffit à convaincre de l'importance de cette activité à leurs yeux. En semaine, 36 % des 16-18 ans passe au moins 3 heures sur un réseau social, et cette proportion atteint les 56 % en dehors des jours de classe.

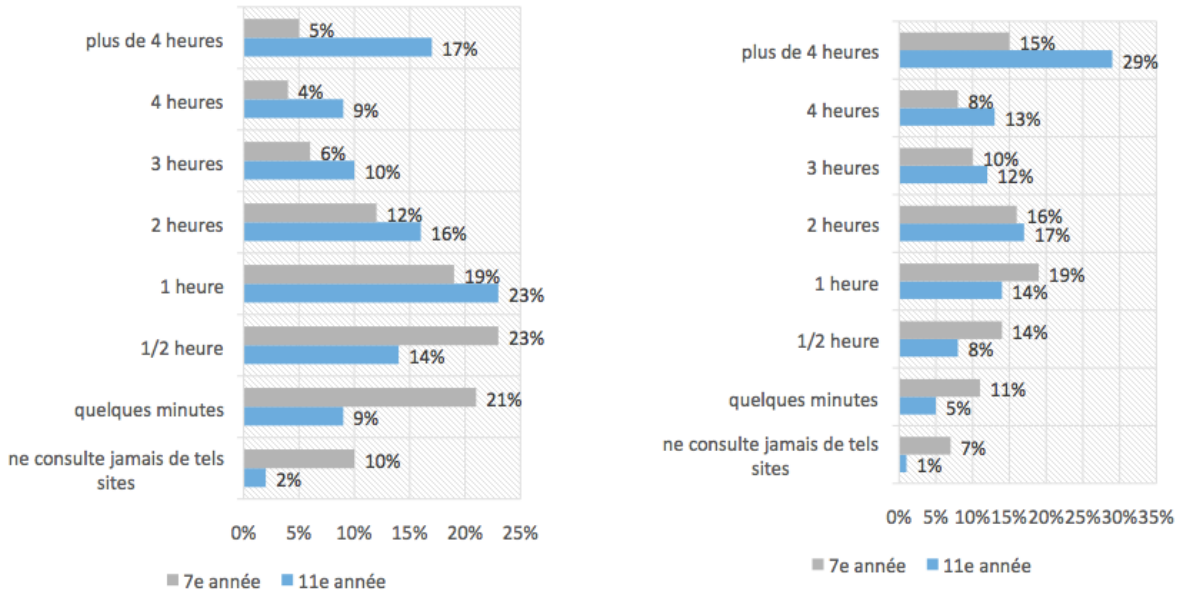


Figure 6 : Temps passé sur un réseau social les jours de classe (à gauche) et les autres jours (à droite)

L'âge joue, comme nous pouvons le voir sur le tableau ci-dessus, un rôle déterminant dans le temps que passent les enfants sur les réseaux sociaux.

Il y encore quelques années, iWiW, MySpace et Facebook dominaient le marché hongrois des réseaux sociaux. Ce paysage s'est aujourd'hui radicalement transformé. Le rôle particulier de Facebook ne peut aujourd'hui faire de doute. Dans le même temps, de nouveaux acteurs présentant des services différent et différemment ont fait leur apparition. Ce n'est donc pas un hasard s'il est presque impossible de trouver dans la population d'étude des jeunes n'ayant aucun compte sur un réseau social. Au total, 8 % d'entre eux n'ont aucun compte sur un réseau social.

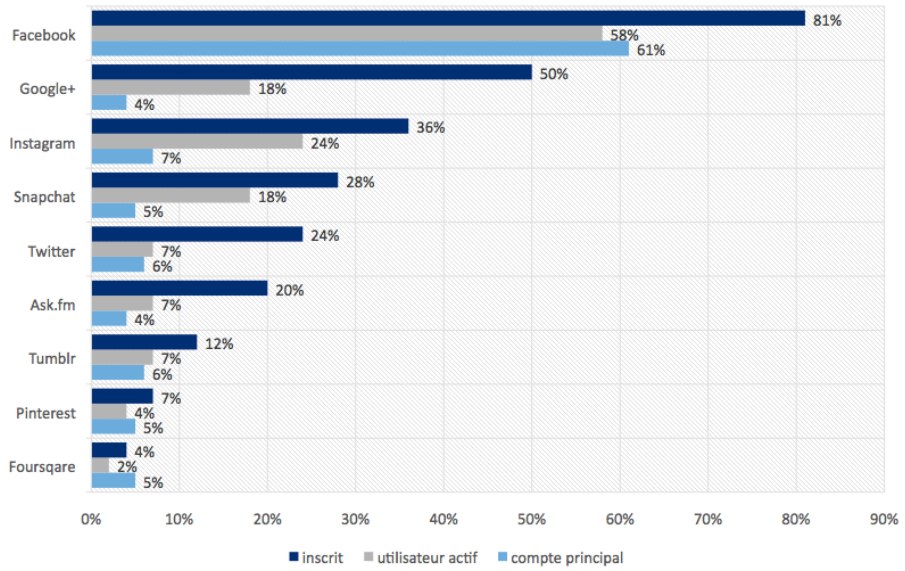


Figure 7 : Comparaison de la popularité de différents réseaux sociaux parmi les élèves de 7e et 11e année

Si 81 % des jeunes disposent d'un compte Facebook, ce dernier n'est le réseau social principal que de 61 % d'entre eux, et seule une proportion encore plus faible, 58 %, s'en considère comme un utilisateur actif.

En moyenne, les jeunes sont inscrits sur 2,8 réseaux sociaux. 18 % d'entre eux disposent d'au moins 5 comptes de réseau social. Les filles ont plus fortement tendance que les garçons à s'inscrire sur un grand nombre de réseaux sociaux, et en particulier, à s'inscrire sur Instagram (43 % des filles, 30 % des garçons) ou Tumblr (17 % de filles contre 9 % de garçons). Par contre, Google+ est plus populaire chez les garçons que chez les filles.

C. Nombre de contacts sur les réseaux sociaux

Il n'est pas évident de déterminer de façon précise le nombre de connaissances sur un réseau social. Au cours de notre étude, nous avons demandé aux enquêtés le nombre d'amis qu'ils avaient sur leur réseau social principal. Sur l'ensemble de l'échantillon, soit sur les deux tranches d'âge étudiées, la moyenne des contacts sur le réseau social principal était de 521.

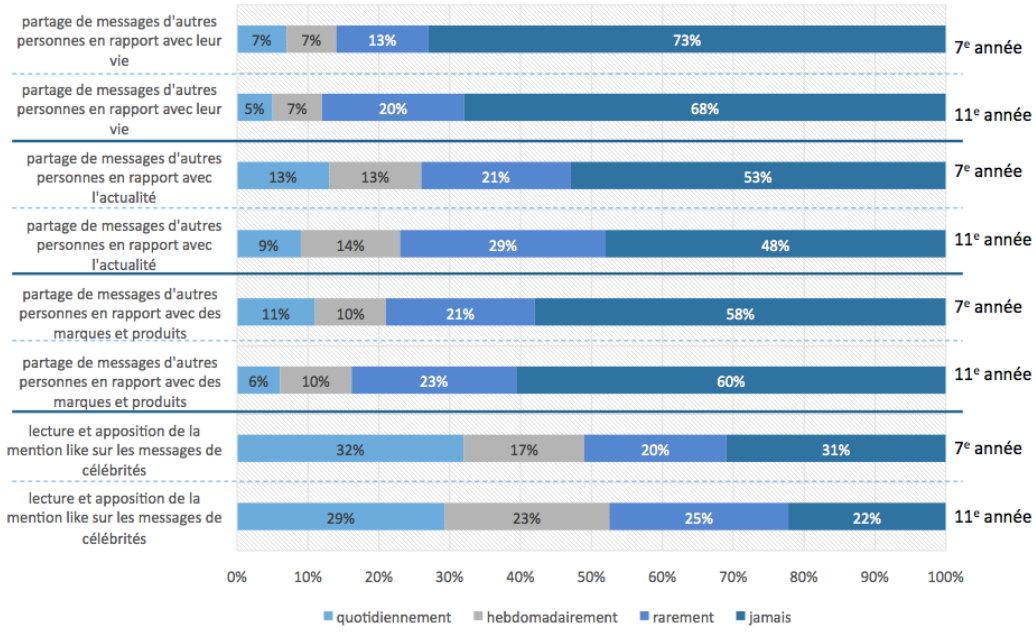
	7e année	11e année
garçon	310	638
fille	341	706

Figure 8 : Nombre de contacts sur le réseau social principal, réparti par tranche d'âge et par sexe

La meilleure façon de gérer une telle quantité de contacts sur un réseau social est de les catégoriser, pour faciliter le contrôle des droits d'accès de tel ou tel groupe aux contenus mis en ligne. Peu d'entre eux font cependant cet exercice : 52 % des jeunes n'utilise pas du tout cette fonctionnalité, 43 % ne classe qu'une partie de ses contacts dans des catégories. 4 % seulement des jeunes classe tous ses contacts dans des catégories.

D. Activités

Comme nous l'avons vu, une large part des « jeunes d'aujourd'hui » passe tous les jours plusieurs heures sur les réseaux sociaux, et ce encore plus le week-end qu'en semaine. Mais que recouvre l'usage des réseaux sociaux ? Les données disponibles ne permettent pas de conclure à une différence notable dans les usages entre les deux tranches d'âge étudiées. Les modes de consommation passifs sont par ailleurs les plus populaires.



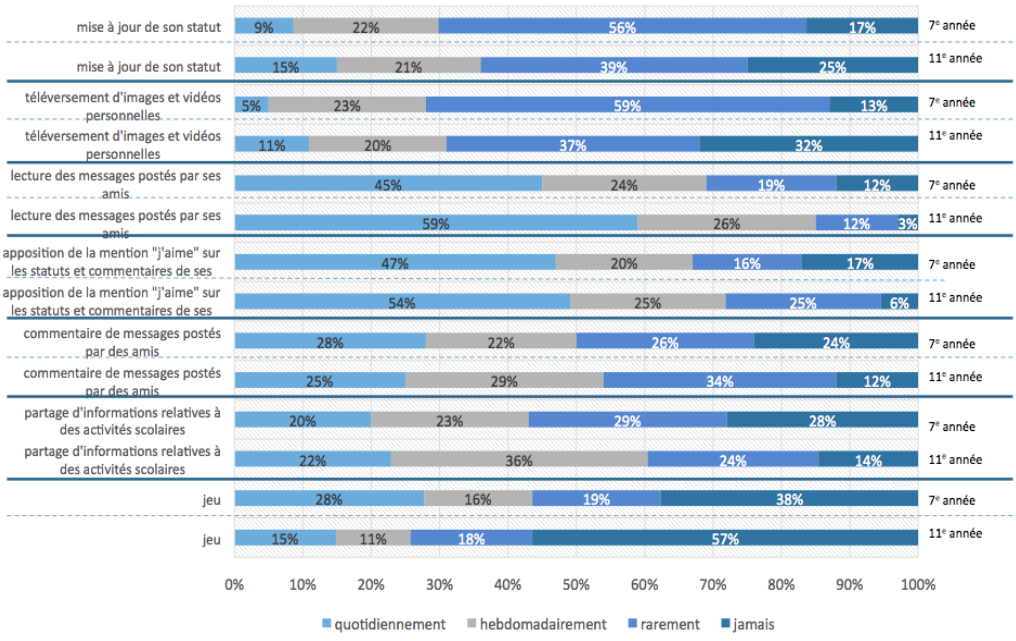


Figure 9 : Usages des réseaux sociaux par type d'activité, tranche d'âge et fréquence de l'activité

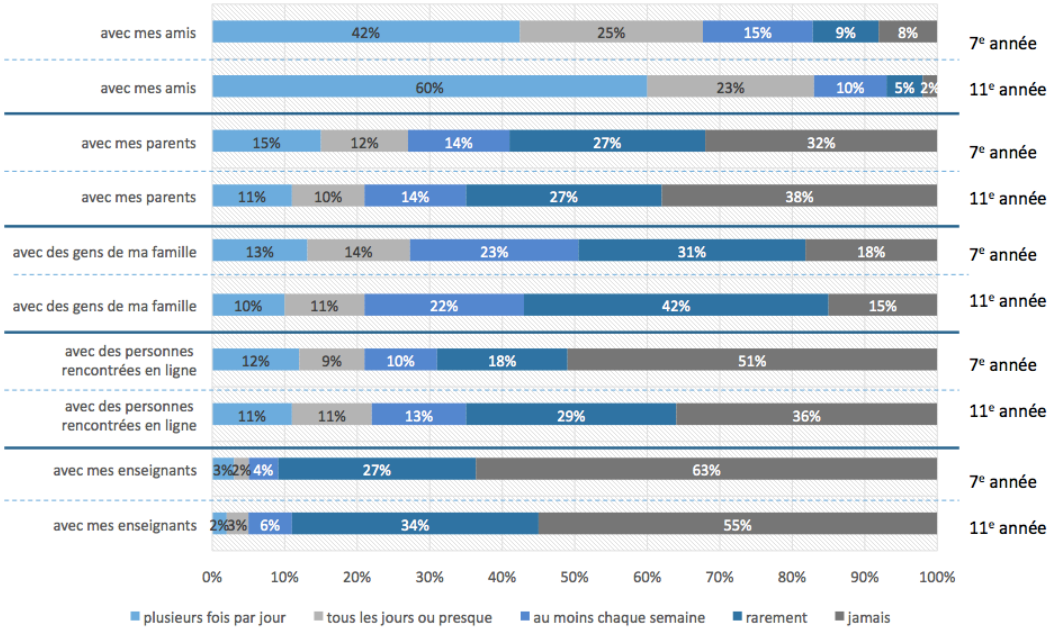


Figure 10 : Personnes avec qui ont lieu les interactions sur les réseaux sociaux

5. L'ENVIRONNEMENT EN LIGNE DES ENFANTS

Les droits des enfants sont inscrits dans la Convention 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 »[16].

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[17].

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

16 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

17 Working document 1/2008 on the protection of children's personal data

6. 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.

Le droit fondamental à la protection des données à caractère personnel a notamment pour rôle de protéger les mineurs eux-mêmes, et non ses parents ou représentants légaux, dont le rôle est de représenter et défendre les intérêts des mineurs concernés. Selon la doctrine du Groupe de travail international sur la protection des données dans les télécommunications (IWGDPT), l'institution du consentement parental peut même, dans certains cas, contrevenir au principe du droit à l'auto-détermination informationnelle[18].

Dans le cas du 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[19], 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, interdits 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[20].

18 « Children's Privacy On Line: The Role of Parental Consent », Working Paper of the IWGDPT, 26 mars 2002
19 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról1
20 Http://index.hu/tech/2013/04/22/gyerekek_es_az_internet/

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 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 »[21].

C. Troubles de la personnalité

La littérature psychologique et psychiatrique[22] s'intéresse 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 avec ses proches de la « vie réelle » ;
- L'immersion dans un espace et un temps virtuel, aboutissant à une perte de contact avec

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

22 Les sources utilisées par dr. Nóra Belső pour la rédaction du présent chapitre sont :
- Cecilie Schou Andreassen (2013). The relationships between behavioral addictions and the five-factor model of personality. Journal of behavioral addictions, 12 avril 2013. 2062-5871
- DEVELOPMENT OF A FACEBOOK ADDICTION SCALE 1, 2. Cecilie Schou Andreassen Psychological Reports, 2012, 100, 2, 501-517. © Psychological Reports 2012 Department of Psychosocial Science University of Bergen, The Bergen Clinics Foundation, Norway
- Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C. & Egloff, B. (2010). Facebook profiles reflect actual personality, not self-idealization. Psychological Science, 21, 372-374

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 ;
- 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.

Les conditions générales d'utilisation de Facebook ont été de nouveau modifiées le 30 janvier 2015. Plusieurs autorités de protection des données ont entamé des procédures de contrôle. En Belgique, l'affaire, portée par l'autorité belge de protection des données, a abouti à un jugement

condamnant cette entreprise pour avoir traqué les comportements de navigation d'internautes sans leur consentement. Lorsque quelqu'un – et cela peut être quelqu'un ne disposant d'un compte Facebook – tombe sur une page web comportant un module d'extension lié à Facebook, comme un bouton « like » ou « partager », Facebook installe sans prévenir sur son ordinateur un cookie (*DATR cookies*) permettant de tracer son historique de navigation. En 2016, le Tribunal de district de Düsseldorf a condamné une grande firme de vêtements de mode à 250 000 euros d'amende (ou, alternativement, 6 mois de prison ferme pour ses dirigeants) pour avoir installé des boutons « Like » sur son site Internet, transmettant ainsi sans le consentement des internautes le consultant des données personnelles à Facebook, en violation avec le droit allemand[23].

Le niveau de publicité des profils dépend du réseau social considéré et des paramètres de confidentialité de la personne concernée. L'existence sur un réseau social débute par le partage de données à caractère personnel. Le minimum est en général le nom de la personne concernée, son âge, son adresse de domicile, ses centres d'intérêt, une courte présentation, souvent une photo de profil, et tout ce que la personne concernée trouve encore d'important à raconter sur soi. La masse de millions de données personnelles mises en ligne et ainsi dévoilées au public entame sérieusement la protection de la vie privée de générations entières, et en premier lieu de celle des jeunes.

Selon une enquête réalisée au niveau européen[24], 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[25].

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.

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[26]. 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.

23 http://www.reuters.com/article/us-facebook-like-germany-idUSKCN0WB1OI

24 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

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

26 CJUE 6 novembre 2003, Aff. C-101/01 « Lindqvist » Rec. I-12992

E. Les contenus nuisibles

De nombreux contenus disponibles sur Internet peuvent, bien qu'ils ne soient pas nécessairement illégaux en eux-mêmes, 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. Ainsi, selon l'étude EU Kids Online de 2014, parmi les Européens de 11 à 16 ans, 20 % sont tombés sur des contenus d'incitation à la haine, 13 % sur des contenus d'incitation à l'anorexie, 11 % sur des contenus incitant à l'auto-mutilation, 12 % sur du contenu harcelant mis en ligne.

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[27]. 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[28].

F. Les moteurs de recherche ou les portes du Net

Les plateformes numériques comme les moteurs de recherche contrôlent l'accès à l'information, et pratiquent souvent une mise à disposition sur mesure en fonction de l'utilisateur. Les internautes hongrois sont entre 93 et 96% à utiliser le moteur de recherche de Google, pour 99% des requêtes[29] en 2014, sans réfléchir à ce que leurs attentes et besoins en matière d'accès à l'information ne sont pas les seuls facteurs déterminants les modalités de mise à disposition de la liste des résultats. Si en effet l'algorithme de Google trie les résultats en fonction des degrés de pertinence pour l'utilisateur, les sommes versées par les annonceurs jouent également un rôle dans l'affichage des résultats. L'ordre d'apparition dans les résultats de moteur de recherche joue en effet un rôle de premier ordre dans la concurrence économique. En effet, les internautes n'ont tendance à cliquer sur des liens figurant parmi les cinq premiers résultats de recherche.

27 Article 77 du Code Pénal hongrois

28 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

29 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf , 2016-02-12

Il est donc nécessaire d'enseigner aux enfants non seulement la technique d'utilisation d'un moteur de recherche, consistant par exemple à savoir trouver les bons mots-clefs à entrer dans une requête, mais aussi un regard critique leur permettant d'évaluer de façon autonome le niveau de qualité des résultats de recherche.

G. Profilage linguistique sur Internet[30]

Les possibilités ouvertes par les nouvelles technologies ont permis l'apparition de nouvelles formes de criminalité. En Hongrie comme à l'étranger, il est difficile de retrouver les auteurs d'actes criminels ou délictueux commis en ligne. Les spécialistes de la langue peuvent aider les services de police à cela en réalisant les profils linguistiques.

Le profilage linguistique est une des branches de la linguistique criminelle. Contrairement au rumeur, elle repose non sur la graphologie mais sur l'analyse textuelle. Nous[31] pouvons établir le profil sociodémographique de quelqu'un pour tenter de déterminer son âge, son sexe, son niveau d'études, ou encore sa langue maternelle. Le profilage linguistique peut notamment s'avérer utile pour casser l'anonymat ou le pseudonymat de l'auteur d'un message.

Bien qu'apparue récemment en Hongrie, la linguistique criminelle, ou criminologie linguistique, n'est pas une science nouvelle dans la littérature internationale. Si les premières publications remontent à 1960, sa pratique n'a commencé à s'implanter que très récemment.

Aux débuts de l'ère numérique, la limitation de la taille des SMS posa des enjeux importants, en imposant aux utilisateurs de cette technologie une double contrainte : limiter la taille du texte tout en faisant parvenir un maximum d'information au destinataire. De là sont nées de nombreuses abréviations, souvent basées sur l'anglais, comme « lol » pour « laughing out loud » (rire à gorge déployée) ou « b4 » pour désigner « before » (avant). Des contraintes similaires s'exercent sur le langage scriptural spécifique au monde du jeu vidéo : il est nécessaire de taper vite au clavier pour communiquer avec ses co-équipiers, car celui qui écrit, ne peut pas jouer en même temps.

Le monde virtuel n'offre pas seulement aux criminels la possibilité de se cacher, mais il facilite leur travail. Pourtant, l'analyse des habitudes linguistiques en ligne a pris du retard.

L'analyse textuelle dans le cadre d'une enquête sur une infraction commise sur Internet consiste en l'analyse de journaux de tchat, en la comparaison de profils Facebook, ou encore en des enquêtes sur des délits d'incitation à la haine. Il faut en cela distinguer les textes publiés en ligne des textes publiés hors ligne, puis mis en ligne. Les textes directement mis en ligne comportent les marqueurs spécifiques du langage du web, que l'enquêteur doit prendre en compte.

Les pratiques linguistiques sur Internet qui forment notre identité linguistique numérique diffèrent de nos pratiques quotidiennes hors ligne. Cela ne veut pas dire que l'identité linguistique numérique gomme les différences individuelles de langage. Ce qui rend unique n'est souvent pas le lexique employé, puisque celui-ci est souvent assez général dans le monde virtuel, mais la façon dont les autres unités linguistiques sont utilisées. Ainsi, nous avons déjà travaillé sur un cas où nous avions pu délimiter un corpus de textes présentant tous le même type d'erreur grammaticale quant à l'emploi d'un affixe particulier. Sur une trentaine de textes étudiés, nous avons ainsi pu attribuer

30 Ce chapitre (qui se trouve ici résumé en français) a été rédigé par la linguiste Sára Ránki

31 Conformément aux conventions de rédaction des publications de recherche, le texte est rédigé à la première personne du pluriel (note de l'auteur)

quatorze d'entre eux à un seul et même auteur. Cette identification est possible car personne n'utilise le langage de façon suffisamment consciente pour en effacer toute trace de sa personnalité, tous ses défauts de langage idiosyncratiques.

Une autre part de l'activité de la linguistique criminelle, à côté de l'analyse de texte et de la constitution de profils sociodémographiques, est l'analyse de pseudonymes. Par exemple, au cours d'une enquête, il nous a été demandé si deux corpus de textes appartenant l'un au pseudonyme « Sebinoka Hai » et l'autre au pseudonyme « Solomon Cedar » pouvaient en réalité appartenir à un seul et même auteur. L'analyse des pseudonymes a révélé les éléments suivants :

- *Sebinoka Hai* : le mot « hai » peut se trouver dans un dictionnaire. Il désigne le requin. Le mot Sebinoka a cependant occasioné quelques maux de tête, car il n'existe dans aucune langue. Le mot « sebino » existe cependant sur une page italienne, et désigne un type particulier de poupée réaliste, à forme humaine, avec des poils humains. Le suffixe « ka » correspond probablement au suffixe diminutif hongrois. Or, il arrive en hongrois d'apposer un suffixe hongrois à un mot étranger. Ainsi, Sebinoka Hai pouvait désigner, selon toute probabilité, un requin mangeur de poupée, ce qui était cohérent avec les autres éléments de l'affaire sur laquelle nous enquêtions.
- Il n'a pas non plus été simple de décoder *Solomon Cedar*. Cette paire de mots ne se trouve que dans une traduction anglaise de la Bible : « So Hiram gave Solomon cedar-trees and cypress-trees [according to] all his desire ». La volonté de se rapprocher de Dieu ou de s'intéresser aux choses spirituelles est fréquente chez des personnes aux comportements linguistiques déviant de la norme. Tout ceci pourrait soutenir la thèse selon laquelle les deux pseudonymes désignent une même personne, dont la pratique linguistique dévie de la pratique générale. L'analyse des textes des corpus renforce cette hypothèse.

Si le Web permet de se cacher derrière l'anonymat, personne ne peut se cacher de sa propre langue.

H. 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. L'Internet ubiquitaire, ou Internet des objets

À l'origine, l'accès à Internet passait impérativement par un ordinateur de bureau. Aujourd'hui se développent une grande 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.

7. PANORAMA DES PRINCIPALES DÉVIANCES SUR INTERNET

Le slogan « si tu le postes pas, ça s'est pas passé » semble diriger la vie quotidienne des jeunes. Ils vivent leur vie sur les plateformes numériques et avec des inconnus virtuels d'une façon qu'il leur semble parfaitement naturelle. Ils ignorent les risques associés jusqu'au jour où ces risques finissent par les rattraper. La situation générale d'anomie, l'apparence d'anonymat, la faiblesse des sanctions des communautés virtuelles et la rupture des conventions sociales habituelles du monde physique sont autant de facteurs qui favorisent l'apparition de nouvelles formes de déviance sur Internet. Nous avons donc procédé à l'analyse des principales formes de ces déviances dans notre étude de 2013, actualisée en 2016[32].

A. Le harcèlement sur Internet

Le harcèlement est le principal facteur de risque auquel 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.

Si en 2010, 7 % des enfants européens de 11 à 16 ans ont fait face à du harcèlement en ligne, ce chiffre avait significativement augmenté en 2014, pour atteindre 12 % de cette tranche d'âge[33]. Les conséquences du harcèlement peuvent être très graves. Selon une enquête de l'Union européenne, 55 % des enfants victimes de harcèlement font état de dépression, 35 % ont porté atteinte à eux-mêmes, et 38 % envisage le suicide comme une solution[34]. Le harcèlement en ligne et le harcèlement hors ligne vont souvent de pair, le premier se poursuivant souvent dans l'école ou dans la rue de la victime, empêchant cette dernière d'y échapper.

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

32 La version intégrale est disponible en anglais ou en hongrois sur notre site Internet
33 http://lsedesignunit.com/EUKidsOnline/index.html?r=64 (page consultée le 22 février 2016)
34 http://europa.eu/epic/news/2014/20140805-cyberbullying-harm-european-children_en.htm (page consultée le 14 janvier 2016)

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[35].

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 « sexting » consiste en l'échange d'images ou de vidéos érotiques à l'aide des outils modernes d'information et de communication. Cette pratique est devenu un phénomène de mode ces dernières années parmi les jeunes.

Selon une étude de 2014, 22 % des adolescentes et 18 % des adolescents a déjà au moins une fois envoyé une image érotique de soi. De plus, 15 % d'entre eux ont déjà envoyé une telle image d'eux à un ou des inconnus[36].

Dans la plupart des affaires qui sont « découvertes », les clichés ont été réalisés avec le consentement de la personne concernée. Mais une fois expédiés et stockés quelque part, leur sort peut devenir totalement indépendant de la volonté du sujet de la photographie ou de la vidéo en question, et peut se retourner contre lui. D'un point de vue technique, rien n'empêche en effet une telle photo ou vidéo d'être reproduite et transférée à l'infini. Le manque de responsabilité, qui consiste à voir en une telle multiplication et diffusion d'images érotiques contre la volonté de la personne concernée une « bonne blague », et le désir de vengeance consécutif à une rupture amoureuse sont les deux principales motivations des agresseurs.

Le cas parvenu à la connaissance de la NAIH illustre bien les problèmes occasionnés par la pratique du sexting : une adolescente de 14 ans et un adolescent de 16 ans ont réalisé des photographies érotiques l'un de l'autre. Le garçon a partagé par vantardise ces photos sur un groupe fermé d'un réseau social auquel appartenaient presque toute la classe. Le père de la fille a pris connaissance des faits et déposé plainte auprès de la police. Les garçons de la classe ont été

35 Http://knowyourmeme.com/memes/events/jessi-slaughter
36 http://nobullying.com/sexting-statistics/ (page consultée le 24 février 2016)

entendus comme témoins par la police au cours de l'enquête, la fille n'ayant jamais donné son consentement au traitement des photographies ou à leur partage. Une des questions à résoudre était de savoir si ceux qui ont vu les clichés les ont transmis à d'autres encore, auquel cas ils s'étaient rendus coupables d'une infraction à la protection des données à caractère personnel. La simple vue d'une image ne constitue en effet pas un traitement de données au sens de la loi.

E. La pédophilie sur Internet

Un pédophile est un adulte attiré sexuellement 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.

Il nous faut enfin parler d'une nouvelle forme d'exploitation des enfants. Il s'agit de la pédophilie virtuelle, par webcam, bien plus sûre et bon marché pour les pédophiles. En 2013, l'association néerlandaise de défense de l'enfance Terre des hommes a identifié mille pédophiles en dix semaines. Ils ont pour cela utilisé un modèle 3D ressemblant à une jeune philippine de dix ans baptisée « Sweetie ». Dans les deux et mois et demi de l'expérience, plus de vingt mille personnes sont entrées en conversation avec elle, parmi lesquelles beaucoup lui ont demandé des services sexuels, certains allant jusqu'à proposer des sommes d'argent. L'association parvint à identifier un millier de pédophiles, généralement grâce à des informations retrouvables sur des médias sociaux. La base de données ainsi constituée a été transmise à Interpol. L'association a tourné un documentaire sur cette action[37].

F. Fausse identité (*grooming*) et prédation

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

37 http://kronika.ro/szines/ezer-pedofilt-fogott-a-virtualis-kislany (page consultée le 5 février 2016)

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.

La prédateurs agissant sur Internet essayent de diverses façons d'entrer en contact avec leurs victimes. Ils peuvent leur faire des propositions alléchantes, leur demander de l'aide ou leur en proposer, faire référence à des amis communs ou à des événements partagés, surveiller les habitudes de leur victime, leur proposer du travail, de l'argent facile, ou encore une carrière de mannequin. Les diverses sortes de réseaux sociaux offrent la possibilité aux prédateurs de connaître les habitudes, les centres d'intérêt voire les données personnelles des internautes mineurs. Il est souvent possible de retrouver facilement où se trouve une personne, ou à quels événements elle compte se rendre dans les jours qui suivent. L'objectif est d'entrer en contact et de construire un lien de confiance, puis de l'approfondir pour que l'enfant se sente dépendant du prédateur au point d'entamer une relation sexuelle, de transférer de l'argent ou des objets de valeur, de réaliser des images ou vidéos pornographiques ou bien de mener des conversations au contenu érotique. Souvent, la victime ne réalise qu'elle a été victime de « grooming » qu'une fois que ces choses sont évoquées, ou ont déjà eu lieu[38].

G. La pratique du *flaming*

Le « flaming » est un des modes opératoires du harcèlement sur Internet. Il s'agit d'une « guerre » virtuelle, par le biais de commentaires agressifs, grossiers et virulents postés sur des forums publics, le plus souvent dans le cadre de débats politiques, religieux ou idéologiques[39]. Les auteurs de tels actes mettent en ligne des commentaires délibérément injurieux et vexants, souvent sans rapport avec le thème initial de la discussion, sur des forums publics, des réseaux sociaux, des blogs personnels, des salons de tchat, des groupes de discussion ou sur des plateformes d'hébergement de vidéos comme YouTube. Les « flamers » sont souvent motivés par leurs propres complexes, agressivité ou manque de confiance. Si certains se sont choisis une cible particulière, par exemple en fonction du genre, de l'origine ethnique ou encore des convictions religieuses de la victime, d'autres cherchent avant tout par ce biais à se divertir.

H. 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[40].

La question des jeux de hasard est simple à trancher d'un point de vue juridique : l'article 1

38 www.kek-vonal.hu/index.php/hu/internetes-biztonsag/212-mi-a-grooming (page consultée le 27 janvier 2015)

39 http://www.kek-vonal.hu/index.php/hu/szolgaltatasok/internetbiztonsag/395-internetes-zaklatas (page consultée le 27 janvier 2015)

40 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

paragraphe 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[41]. La même année, le chiffre d'affaire total du marché du jeu vidéo dans ce pays atteignait les deux milliards d'euros.

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 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 il existe un phénomène de « criminalité virtuelle » : il arrive que des joueurs évoluant dans un monde virtuel – typiquement en jouant à un jeu de rôle en ligne massivement multijoueur (ou MMORPG) – harcèlent d'autres joueurs du même monde, ou y commettent des actions en jeu visant à porter atteinte aux intérêts matériels des autres joueurs. Ces intérêts matériels recouvrent des biens virtuels échangés sur des marchés simulés dans ces jeux, qui ont un impact aussi sur l'économie réelle[42]. Un exemple classique de vol de bien virtuel s'est déroulé

41 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

42 Edward Castronova: On Virtual Economies. Gamestudies.org, décember 2003. http://www.gamestudies.org/0302/castronova

au Japon : un individu y avait abusé de la confiance d'un joueur lui ayant confié ses identifiant et mot de passe pour revendre 50 000 yens, sur eBay, la « maison » virtuelle dans laquelle vivait l'avatar du joueur[43]. Lorsque les conditions générales d'utilisation d'un jeu simulant un monde virtuel y autorise les joueurs, ils peuvent revendre les biens virtuels acquis au cours d'une partie. Dès lors, il est à noter que ces biens deviennent juridiquement des biens dont la jouissance est cessible. Le fait d'entraver la jouissance d'un tel bien devient alors juridiquement répréhensible[44]. Cette situation est à distinguer des cas où le joueur se met de lui-même et volontairement dans une situation de jeu au cours de laquelle des biens virtuels utilisés dans le jeu peuvent être détruits. Par exemple, début 2014, entre 70 et 114 millions de dollars US de biens virtuels ont été détruits au cours d'une guerre virtuelle s'étant déroulée dans un jeu de plusieurs millions d'utilisateurs se déroulant dans un univers de science fiction[45].

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[46].

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 gratuits ; 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

43 Slashdot.org: Japanese Man Arrested for Virtual Theft. 14 février 2003. http://www.slashdot.org/articles/03/02/14/0523248.shtml?tid=127

44 Dániel Eszteri: A World of Warcraft-tól a Bitcoin-ig: Az egyén a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Thèse de doctorat, Université des Pécs, Faculté de droit et de science politique. http://alk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-vedes-ertekezes.pdf

45 HVG.hu: A neten kívül is hatalmas károkat okozott 24 óra alatt egy netes háború. 30 janvier 2014. http://hvg.hu/tudomany/20140130_hatalmas_karokat_okozott_egy_netes_haboru

46 http://mediasmarts.ca/blog/game-tips-parents 15 avril 2013

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[47].

47 http://www.penzcentrum.hu/vasarlas/tizezreket_bukhatnak_a_gyanutlan_vasarlok_tamadnak_az_atveros_netes_boltok.1035976.html ,15 mai 2013

8. 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.

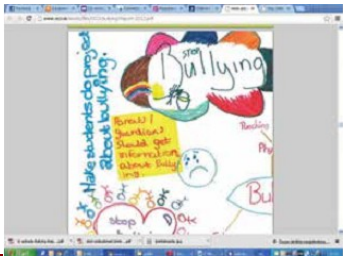
Reconnaissant l'importance du sujet et le succès du projet, le Ministère de l'Éducation a introduit en 2012 la question des données personnelles dans le programme national d'éducation aux TIC à destination des collégiens.

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[48]. 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



48 http://dataprotection.ie/viewdoc.asp?docID=520

réseaux sociaux : http://www.thejournal.ie/safebook-how-to-stay-safe-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. Pologne : Programme « Your Data – Your Concern »

L'autorité polonaise de protection des données (GIODO), le Centre Pédagogique de Gliwice, le Ministère de l'Enseignement et le Médiateur du droit des enfants ont publié ensemble un guide destiné aux enseignants et professionnels de l'éducation. L'objectif principal était de produire un outil capable d'améliorer le niveau de compétence des enseignants en matière de protection de la vie privée sur Internet et de protection des données à caractère personnel, en vue d'une intégration dans les programmes scolaires d'une sensibilisation à ces questions. Le produit final du projet Your Data – Your Concern (Tes Données, Ta Responsabilité) comportait à la fois des informations, mais aussi des kits pédagogiques déployables en classe et visant une tranche d'âge allant de 7 à 16 ans.

F. France : « Plus de droits pour vos données ! »

La CNIL a publié des ressources à destination des professionnels de l'éducation et des adolescents. Elle a aussi publié une page intitulée « Plus de droits pour vos données ! » qui présente sous forme de dessins ludiques les principaux aspects de la réforme européenne du droit des données personnelles, qui ouvre de nouveaux droits pour les personnes concernées[49].

G. Espagne : Projet PANDI[50]

L'autorité espagnole de protection des données (AEPD) a construit une campagne de communication à destination des jeunes sous la forme d'une bande dessinée mise en ligne sur un portail dédié. Cette bande dessinée raconte l'histoire d'un groupe d'amis. Elle apprend aux enfants l'importance de la protection des données et de penser de façon critique. Le site Internet comporte six modules pédagogiques transmettant des connaissances de base et proposant des études de cas.

H. 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.

49 https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
50 http://tudecideseninternet.es/menores-v2/?q=node/176

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

I. 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.

J. États-Unis d'Amérique

En 1998, le Congrès américain a adopté le Children's Online Privacy Act (COPPA)[51], 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[52].

51 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).

52 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[53].

Le réseau Insafe, qui participe à l'organisation du « Safer Internet Day », a publié à l'occasion de l'édition 2013 de l'événement des manuels intitulés « A Web We Want »[54], l'un étant destiné aux adolescents, et l'autre aux éducateurs. Ces manuels sont de précieux outils pour les enseignants et éducateurs qui souhaitent intégrer à leurs cours une formation au bon usage du web.

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 .

53 www.saferinternet.hu
54 http://www.webwewant.eu/fr/web/guest/get-the-www

9. 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

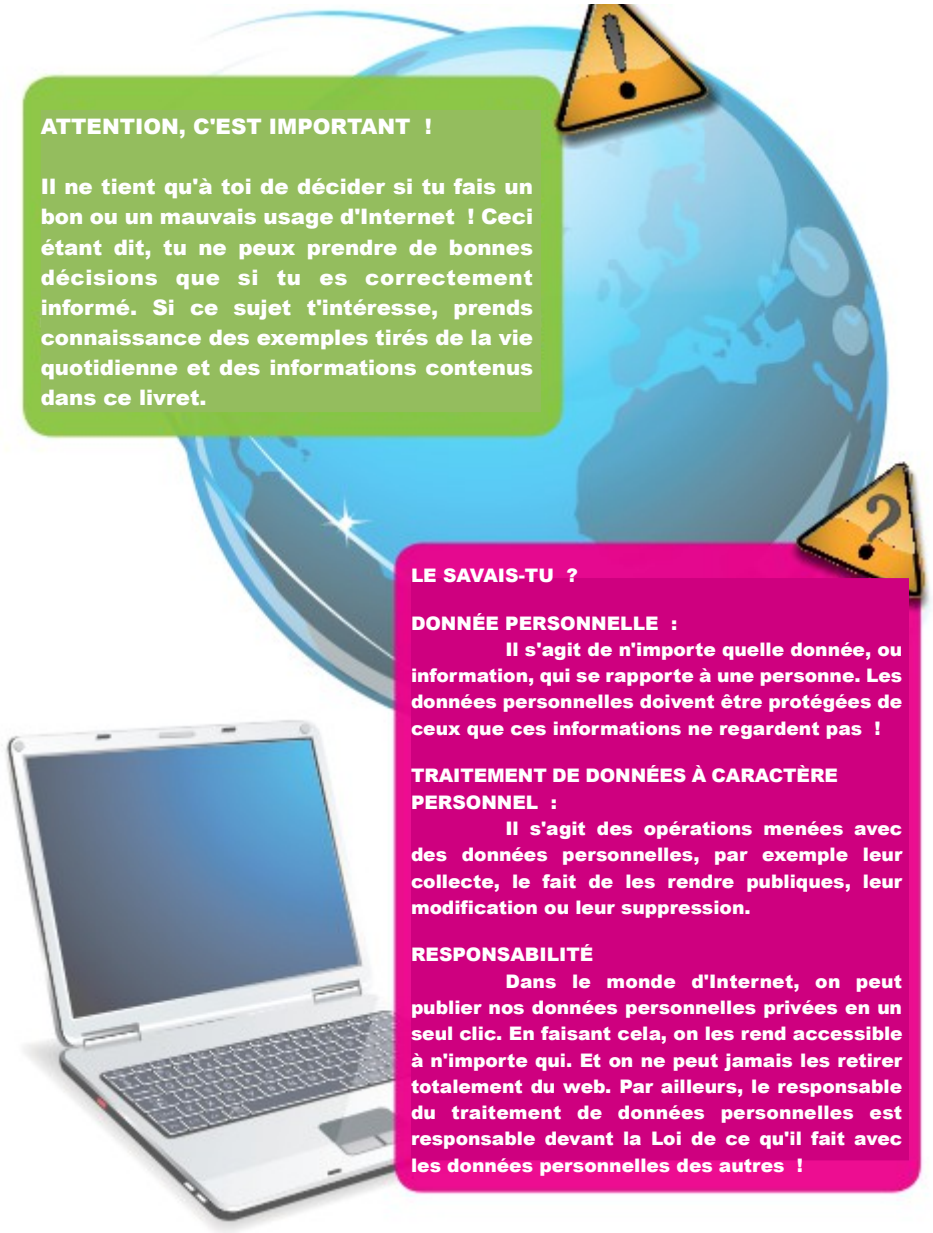
Poèmes

- *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

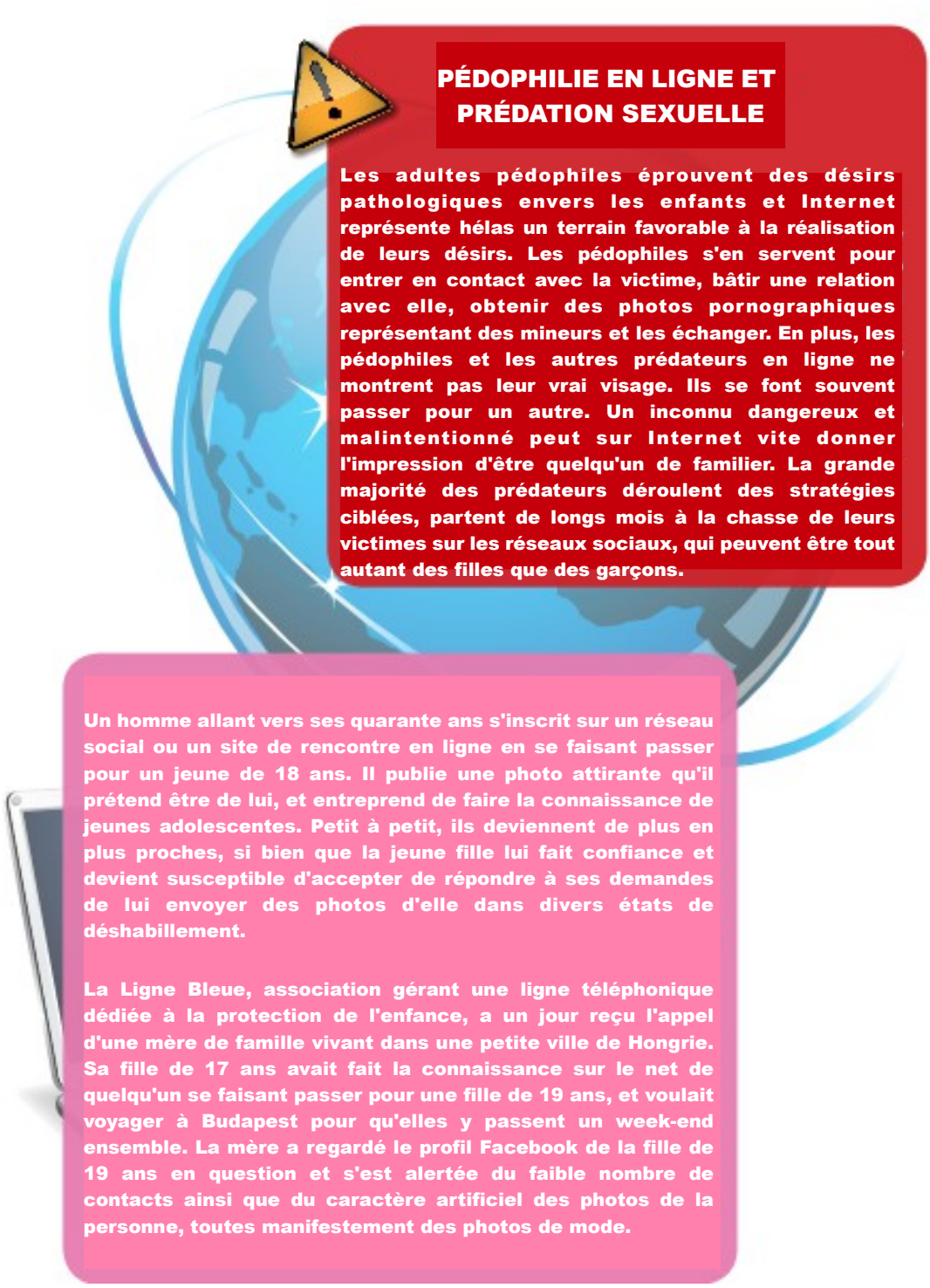
Chat, ou encore clavardage. C'est ce qu'on dit quand deux personnes ou plus dialoguent en temps réel à travers un canal (en anglais chatroom) auquel ils ont accès via un programme spécialement dédié.

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 !