Mémorandum sur le droit à la protection des renseignements personnels et la vie privée dans les réseaux sociaux sur l'Internet, en particulier ceux des enfants et des adolescents

Mémorandum de Montevideo

CONSIDÉRATIONS GÉNÉRALES

La société de l'information et de la connaissance, avec des outils tels que l'Internet et les réseaux sociaux numériques, constitue une opportunité inestimable pour l'accès à l'information et l'échange d'information, la diffusion des idées, la participation citoyenne, l'amusement et l'intégration sociale, notamment à travers les réseaux sociaux.

Les enfants et les adolescents ont de plus en plus d'accès aux divers systèmes de communication qui leur permettent de tirer profit de tout ce qu'ils représentent ; mais cette situation a aussi poussé à l'extrême l'équilibre entre l'exercice des droits fondamentaux et les risques –pour la vie privée, l'honneur, la réputation et l'intimité, parmi d'autres– qui, de même que les abus qu'ils peuvent souffrir –discrimination, exploitation sexuelle, pornographie, etc.–, peuvent avoir un impact négatif sur leur développement intégral et leur vie adulte.

En Amérique Latine et aux Caraïbes, ainsi que dans d'autres régions, des efforts sont faits au sein de la diversité sociale, culturelle, politique et réglementaire existante en vue d'atteindre un consensus et une rationalité de sorte de créer un équilibre entre la garantie des droits et la protection face aux risques dans la société de l'information et de la connaissance. Dans ce sens, il est possible de citer certains des documents les plus récents : L'*Accord qui met fin à la dispute judiciaire entre le Ministère Public Fédérale du Brésil et Google* (du 1er juillet 200);[1] l'*Initiative de protection des enfants en ligne* de l'Union Internationale de Télécommunications (du 18 mai 2009);[2] l'*Opinion 5/2009 sur les réseaux sociaux en ligne*, du Groupe Européen de Travail de l'Article 29 (du 12 juin 2009);[3] le *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. / Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.*[4] (du 16 juillet 2009).[5]

1. http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/
2. http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html
3. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf
4. http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm

Les recommandations présentées ci-dessous constituent une contribution pour que les divers acteurs de la région y impliqués s'engagent dans ce sujet pour élargir les aspects positifs de la Société de l'information et de la connaissance, y compris l'Internet et les réseaux sociaux numériques, ainsi que pour prévenir les pratiques préjudiciables qui seront très difficiles à modifier, de même que les impacts négatifs qu'elles provoquent.

Toute approche à ce sujet doit considérer deux dimensions. D'une part, la reconnaissance du fait que les enfants et les adolescents sont titulaires de tous les droits et, donc, ils peuvent les exercer en fonction de leur âge et leur maturité, en plus du fait que leurs opinions doivent être prises en considération en fonction aussi de leur âge et leur maturité ; d'autre part, le fait qu'en raison de leur condition particulière de développement, ils ont droit à une protection spéciale dans certaines situations qui peuvent s'avérer négatives pour leur développement et leurs droits.

Le droit à la vie privée est une valeur que toute société démocratique doit respecter. En conséquence, afin d'assurer l'autonomie des individus, de décider la portée de leur vie privée, il faut limiter tant le pouvoir de l'État que celui des organisations privées pour restreindre les intrusions illégales ou arbitraires dans cette sphère personnelle. En particulier, il faut protéger les informations personnelles des enfants et des adolescents sans affecter leur dignité en tant que personnes, car ils ont une expectative de confidentialité raisonnable lorsqu'ils partagent leur information dans des environnements numériques, vu qu'ils considèrent qu'ils se trouvent dans un espace privé.

Dans ce sens, il faut rappeler l'importance de consulter les enfants et les adolescents et de prendre leurs opinions en considération dans les mesures à appliquer dans ce sujet.

La société civile espère des agents économiques la déclaration d'adhésion aux principes, aux attitudes et aux procédures qui garantissent les droits des enfants et des adolescents dans la Société de l'information et de la connaissance.

---

5. D'autres documents spécialement considérés : *Résolution sur la protection de la vie privée dans les services de réseaux sociaux* (Strasbourg, le 17 octobre 2008) ; «Recommandation sur les réseaux sociaux» de l'Agence espagnole de protection des données, « Rapport sur la protection des données personnelles et la sécurité de l'information des réseaux sociaux en ligne », fait par l'Institut National des Technologies de la Communication, INTECO et par l'Agence Espagnole de Protection des Données (2009), la *Déclaration et appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents* (novembre 2008), le Rapport 2/2009 sur la protection des renseignements personnels des enfants du Groupe de Travail Européen de l'Article 29 (2009) ; le Rapport d'Analyse et des Propositions en matière d'accès à l'information et la confidentialité en Amérique Latine du Moniteur de confidentialité et d'accès à l'information, et les documents d'eLAC 2007 et 2010.

Quant à l'éradication de la pornographie infantile sur l'Internet, un effort conjoint de tous les acteurs responsables –des gouvernements, de la police, des fournisseurs d'accès et de contenu, de la société civile, du secteur privé– est souhaitable à l'échelle nationale, régionale et internationale pour mobiliser et impliquer un nombre de plus en plus grand d'entreprises, d'organisations publiques et de la société civile.

Les particularités de genre et la diversité culturelle en Amérique Latine et aux Caraïbes ont été prises en considération pour ces recommandations, ainsi que la diversité des politiques et des réglementations dans la manière de faire face au phénomène de la Société de l'information et de la connaissance, mettant notamment l'accent sur l'Internet et les réseaux sociaux.

Les organismes multilatéraux devront inclure les enfants et les adolescents en tant que sujets spécialement protégés et vulnérables par rapport au traitement de leurs données personnelles dans leurs documents, leurs directives ou leurs recommandations. De même, ils devront concentrer leurs efforts pour favoriser ou renforcer une culture de protection des données chez les enfants et les adolescents.

Ces recommandations se basent, notamment du point de vue réglementaire, sur la Convention des Nations Unies relative aux droits de l'enfant (CDE), un instrument ratifié par tous les pays de la région, où la responsabilité partagée par la société et par l'État, chacun dans son domaine respectif, dans la protection de l'enfance et l'adolescence, est clairement reconnue. Et ce, à partir de trois considérations fondamentales : la reconnaissance du rôle pertinent qui joue la famille –ou les personnes chargées de la garde des enfants et des adolescents– dans le processus d'éducation sur l'utilisation responsable et sûre des outils comme l'Internet et les réseaux sociaux numériques et dans la protection et la garantie de leurs droits ; le besoin que toutes les mesures à prendre donnent la priorité à l'intérêt supérieur des enfants et des adolescents, tout en gardant un équilibre entre les besoins de protection contre la vulnération de leurs droits et l'utilisation responsable de ces outils qui représentent des formes d'exercice de leurs droits ; et que toute personne qui tire profit, quel qu'il soit, de l'Internet et des réseaux sociaux numériques est responsable des services fournis et, en conséquence, doit assumer sa responsabilité vis-à-vis des solutions aux problèmes que ceci entraîne.

RECOMMANDATIONS AUX ETATS ET AUX ETABLISSEMENTS EDUCATIFS POUR LA PREVENTION ET L'EDUCATION DES ENFANTS ET DES ADOLESCENTS

Toute action en matière de protection des renseignements personnels et de la vie privée des enfants et des adolescents[6] doit considérer le principe de

6. Les expressions enfants et adolescents sont utilisées dans le sens que chaque pays leur donne dans la législation nationale. (Selon chaque pays, l'expression «enfants» pourra faire référence aux personnes de moins de 12 ou 13 ans, et «adolescent» aux personnes de plus de 13 ans mais de moins de 18 ans. Dans les pays où la catégorie «adolescents» n'a pas été incluse dans le cadre juridique, elle s'applique aux «mineurs pubères». Dans le cas de

l'intérêt supérieur[7] et l'article 16 de la CDE qui détermine que: «(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.»*

La prévention —sans laisser de côté une approche de politiques, normative et judiciaire— est prioritaire pour faire face aux aspects de la Société de l'information et de la connaissance, en particulier de l'Internet et des réseaux sociaux numériques, identifiés comme risqués, notamment à travers l'éducation, en considérant la participation active des enfants et des adolescents, leurs parents ou d'autres personnes à la charge de leur garde, et les éducateurs, prenant en considération comme principe fondamental l'intérêt supérieur des enfants et des adolescents.

Dans ce but il faut prendre en considération les recommandations suivantes:

1. Les États et les établissements éducatifs doivent tenir compte du rôle des parents ou des personnes responsables de la garde des enfants ou des adolescents dans leur formation personnelle, y compris l'utilisation responsable et sécuritaire de l'Internet et des réseaux sociaux numériques. L'État et les établissements éducatifs doivent fournir l'information et renforcer les capacités des parents et des personnes responsables sur les risques éventuels qui peuvent rencontrer les enfants et les adolescents dans les environnements numériques.

2. Toute mesure qui implique un contrôle des communications doit respecter le principe de proportionnalité ; en conséquence, il faut déterminer que son objectif est la protection et la garantie des droits, qu'elle est appropriée pour le but recherché et que c'est la seule qui permet d'obtenir ces résultats tout en étant la moins restrictive des droits.

3. Il faut transmettre clairement aux enfants et aux adolescents que l'Internet n'est pas un espace sans normes, impuni ou sans responsabilités. Il faut les avertir pour qu'ils ne soient pas trompés par l'apparente sensation que dans l'Internet tout est valable, car toutes les actions ont des conséquences.

Il faut les éduquer dans l'utilisation responsable et sécuritaire de l'Internet et des réseaux sociaux numériques. En particulier :

3.1. La participation anonyme ou l'utilisation de pseudonymes est possible dans les réseaux sociaux numériques. Le processus éducatif doit réfléchir

---

l'Honduras, «enfant garçon» est la personne de moins de 14 ans et «enfant fille» la personne de moins de 12 ans; «adolescents» sont les personnes de plus de ces âges et de moins de 18 ans).

7. Article 3.1 de la CDE «Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale. »

sur les aspects positifs de l'utilisation de pseudonymes comme un moyen de protection et d'une utilisation responsable qui implique, parmi d'autres choses, de ne pas les utiliser pour tromper ou pour confondre les autres sur leur identité réelle.

Les enfants et les adolescents doivent être avertis sur la possibilité que, même s'ils croient être en communication ou partager des informations avec une personne déterminée, en réalité il peut s'agir d'une autre personne. En même temps, il faut leur avertir que la participation anonyme ou avec un pseudonyme rend possible le vol d'identité.

3.2. Pendant le processus éducatif il faut mettre l'accent sur le respect de la vie privée, de l'intimité et de la réputation des tierces personnes, parmi d'autres sujets. Il est important que les enfants et les adolescents sachent que ce qu'ils peuvent divulguer peut enfreindre leurs droits et ceux de tiers.

3.3. Les enfants et les adolescents doivent savoir que la distribution de contenus interdits par la réglementation locale ou régionales (notamment la pornographie infantile), l'harcèlement (notamment l'harcèlement sexuel), la discrimination, l'incitation à la haine raciale, la diffamation, la violence, etc. sont illégaux sur l'Internet et sur les réseaux sociaux numériques et ils sont punis par la loi.

3.4. Le processus éducatif doit apprendre aux enfants et aux adolescents l'utilisation responsable et sûre des politiques de confidentialité, de sécurité et des alertes des instruments d'accès et des sites web qu'ils utilisent fréquemment tels que les réseaux sociaux numériques.

3.5. Il faut promouvoir une politique éducative –exprimée de façon compréhensible pour l'âge des enfants et des adolescents– qui comprenne une stratégie d'information et de formation pour les aider à gérer les potentialités et les risques causés par la Société de l'information et de la connaissance, notamment de l'utilisation de l'Internet et des réseaux sociaux numériques.

3.6.. Il faut également les informer sur les mécanismes de protection et les responsabilités civiles, pénales ou administratives existantes lorsque leurs propres droits ou ceux des tiers sont enfreints dans le réseau.

3.7. Il faut leur avertir du danger qui suppose le vol et/ou la substitution d'identité qui peut se produire aux environnements numériques qui induisent en tromperie.

3.8. Il faut expliquer aux enfants et aux adolescents, en utilisant un langage facile à comprendre, l'esprit des lois sur la protection des données personnelles et la protection de la vie privée de sorte qu'ils puissent saisir l'idée de l'importance du respect de la confidentialité des informations personnelles d'eux-mêmes et des autres.

3.9. Il faut éduquer à propos de l'incertitude sur la véracité des contenus et la validation des sources d'information. Les enfants et les adolescents doivent apprendre à chercher et à discriminer les sources.

4. La promotion d'une éducation continue et complète sur la Société de l'information et de la connaissance est fermement recommandée, notamment pour l'utilisation responsable et sûre de l'Internet et des réseaux sociaux numériques, en particulier à travers:

4.1. L'inclusion dans les cursus, à tous les niveaux éducatifs, des informations de base sur l'importance de la vie privée et la protection des renseignements personnels, ainsi que des autres aspects indiqués au point 3.

4.2. La production de matériel didactique, notamment des audiovisuels, des pages web et des outils interactifs (tels que des jeux *en ligne*) où il y ait des potentialités et des risques. Ces matériels devront comprendre des informations sur les mécanismes de protection des droits

La nature de ces sujets et des ces matériels demande la participation et le débat de tous les acteurs concernés afin de répondre aux particularités locales et culturelles.[8]

4.3. Les enseignants doivent être formés pour faciliter la discussion et placer dans son contexte les avantages et les risques de la société de l'information et de la connaissance, notamment de l'Internet et des réseaux sociaux numériques ; dans ce but, ils peuvent recevoir le soutien des autorités de protection des renseignements personnels ou de toutes les organisations qui travaillent dans ces sujets dans les différents pays.

4.4. Les autorités éducatives –avec l'appui des autorités de protection des données (là où elles existent), du secteur académique, des organisations de la société civile, du secteur privé et, si nécessaire, avec la coopération internationale– doivent aider les enseignants et appuyer le travail dans les domaines décrits.

5. Les autorités compétentes doivent créer des mécanismes pour que les établissements éducatifs puissent résoudre les conflits provoqués par l'utilisation de l'Internet et des réseaux sociaux numériques par les enfants et les adolescents, avec un sens didactique, en considérant toujours l'intérêt supérieur de ces enfants et adolescents, sans enfreindre aucun droit ou garantie, en particulier le droit à l'éducation.

---

8 Liste de contrôle #3 et #4 des **Lignes directrices de l'ITU pour les Décideurs**: « … *Il est très important, donc, que des matériels qui reflètent les lois et les normes culturelles locales soient produits à l'échelle locale. Ceci sera essentiel pour toute campagne de sécurité dans l'Internet ou tout matériel de formation qui soit développé.» ;* 4. *« … Lorsque des matériels didactiques sont produits, il est important de prendre en compte que de nombreuses personnes qui viennent de connaître cette technologie ne se sentiront pas à l'aise en l'utilisant. Pour cette raison, il est important d'assurer que des matériels de sécurité soient mis à la disposition par écrit ou produits en utilisant d'autres moyens avec lesquels les nouveaux venus se sentiront plus à l'aise, par exemple, des vidéos.»*

RECOMMANDATIONS AUX ÉTATS SUR LE CADRE LÉGAL

Le cadre légal qui règle la Société de l'information et de la connaissance dans la région –en particulier l'Internet et les réseaux sociaux numériques– avance lentement par rapport au développement de nouvelles applications et contenus ; il a une série de vides juridiques et de tensions importantes en ce qui concerne la façon de protéger les divers droits. Cependant, il existe un certain niveau de consensus sur le fait qu'il y a assez de principes fondamentaux et constitutionnels pour éclairer les décisions à prendre dans ce domaine.

La création, la réforme ou l'harmonisation réglementaire doivent se faire prenant comme considération essentielle l'intérêt supérieur des enfants et des adolescents, notamment il faut considérer que :

6. La protection des données personnelles demande le développement d'une réglementation nationale, applicable tant au secteur public qu'au secteur privé, qui contienne les droits et les principes fondamentaux reconnus internationalement et les mécanismes en vue de leur application effective. Pour la création et le développement de ces réglementations les États devront prendre spécialement en considération les enfants et les adolescents.

7. Il faut s'assurer que toute action ou omission contre un enfant ou un adolescent, considérée illégale dans le monde réel, reçoive le même traitement dans le monde virtuel, en garantissant toujours leur bienêtre et la protection intégrale de leurs droits.[9]

8. Les États doivent légiférer sur le droit des enfants et des adolescents, directement ou par l'intermédiaire de leurs représentants légaux, à demander l'accès à l'information sur eux-mêmes qui se trouve dans des bases des données tant publiques que privées, à rectifier ou à éliminer cette information si nécessaire, ainsi qu'a s'opposer à son utilisation à quelque fin que ce soit.

9. Il faut développer une réglementation adéquate pour le fonctionnement des centres d'accès à Internet (publics et privés) qui peut comprendre, par exemple, l'obligation d'utiliser des messages d'avertissement, des filtres de contenu, l'accessibilité pour des enfants et des adolescents, etc.

RECOMMANDATIONS POUR L'APPLICATION DES LOIS PAR LES ÉTATS

Pendant les dernières années il y a eu de nombreux conflits ou violations des droits comme conséquence de la diffusion de renseignements personnels, de l'invasion de la vie privée, des diffamations sur l'Internet et les réseaux sociaux numériques qui ont été portés devant les Tribunaux de Justice. Certaines décisions ont montré le rôle des juges pour prendre des

9 **Lignes directrices de l'ITU pour les Décideurs** #2: «*Établir*, mutatis mutandis, *que tout acte contre un enfant qui soit illégal dans le monde réel soit illégal en ligne, et que les règles de confidentialité et de protection des données pour des mineurs devant la loi soient aussi applicables.*»

décisions devant des situations nouvelles sur la base des principes fondamentaux. Cependant, la proportion de conflits qui ont un accès réel à la justice est minime.

Les systèmes judiciaires jouent un rôle très important pour assurer la bonne utilisation d'Internet et des réseaux sociaux numériques. Les sanctions civiles et pénales doivent être appliquées non seulement pour rectifier les droits enfreints mais aussi pour fournir aux citoyens et aux entreprises des règles claires sur l'interprétation des lois et des principes fondamentaux.[10]

10. Il faut garantir:

10.1. L'existence de processus judiciaires et administratifs simples, agiles, d'accès facile, dont les démarches soient prioritaires pour les tribunaux et les autorités responsables.[11]

Il faut renforcer l'utilisation de la responsabilité civile extracontractuelle objective comme mécanisme régulateur pour garantir les droits fondamentaux dans les applications dans la Société de l'information et de la connaissance, l'Internet et les réseaux sociaux numériques. Les sanctions judiciaires pour les dommages provoqués ont l'avantage d'être une réponse immédiate, efficace et capable de dissuader les conceptions dangereuses. Ce type de responsabilité civile est fondé sur l'intérêt supérieur de l'enfant.

10.2. Les décisions à prendre à ce sujet devraient être largement diffusées par l'intermédiaire de techniques d'anonymat qui garantissent la protection des renseignements personnels.

10.3. Il faudrait développer et diffuser une base de données sur des cas et des décisions prises (des jugements judiciaires ou des décisions administratives rendus anonymes) liée à la Société de l'information et de la connaissance, notamment à l'Internet et aux réseaux sociaux numériques; cette base de données serait un instrument pour que les juges puissent apprécier le contexte national et international où ils se trouvent.

11. Il faut créer un canal de communication qui permette aux enfants et aux adolescents de déposer les plaintes pouvant apparaître comme conséquence de la violation de leurs droits en matière de protection des renseignements personnels.

---

10 Déclaration de Principes sur la Liberté d'Expression, de la Commission Interaméricaine des Droits de l'Homme de l'O.E.A. (Octobre 2000) : "10. Les lois sur la protection des renseignements personnels ne doivent ni empêcher ni limiter la recherche et la diffusion d'information d'intérêt public. La protection de la réputation doit être garantie seulement par le biais de sanctions civiles, dans les cas où la personne lésée est un fonctionnaire public ou une personne publique ou un particulier qui a volontairement joué un rôle dans des affaires d'intérêt public. En outre, dans de tels cas, il doit être établi que par la diffusion des avis, le communicateur avait l'intention d'infliger un dommage, qu'il était pleinement conscient de diffuser des informations fausses ou qu'il a fait preuve de négligence manifeste dans la recherche de la vérité ou de la fausseté de ces informations. » [Approuvée pendant la 108º Période Ordinaire de Sessions de la CIDH]

11 Dans ce sens il faut signaler l'intervention des *Tribunaux Spéciaux* du Brésil dans la protection des droits des citoyens aux réseaux sociaux dans l'Internet.

12. Il faut encourager la création d'organismes juridictionnels spécialisés en matière de protection des données.

13. Il faut renforcer des capacités chez les acteurs juridiques impliqués en matière de protection des données, mettant notamment l'accent sur la protection des enfants et des adolescents.

RECOMMANDATIONS EN MATIÈRE DE POLITIQUES PUBLIQUES

Nous rappelons qu'il est nécessaire que l'intérêt supérieur de l'enfant soit considéré comme principe recteur de toute mesure à prendre à ce sujet, notamment en ce qui concerne le développement de politiques publiques visant à réglementer les réseaux sociaux numériques.[12]

14. Il est recommandé de considérer l'application des politiques publiques suivantes:

14.1 La création de mécanismes de réponse pour assister les victimes d'abus dans la Société de l'information et de la connaissance, notamment dans l'Internet ou les réseaux sociaux numériques. Il faut créer également des systèmes d'information pour que les enfants et les adolescents qui aient un souci par rapport aux contenus dans l'Internet ou les réseaux sociaux numériques puissent avoir du conseil et du soutien rapidement.

Dans ce but, il est possible de créer des mesures telles que de l'aide et des plaintes en ligne, des numéros de téléphone gratuits, des centres d'assistance, etc.

14.2. La création de protocoles pour canaliser les contenus illégaux informés.[13]

15. Il faudrait qu'il y ait des mécanismes régionaux et internationaux pour partager les informations dénoncées par des particuliers sur ces événements, en temps réel, afin de pouvoir générer des politiques et des mécanismes de protection de façon précoce, étant donné que les risques

---

12. **Opinion 5:** 4. «L'Opinion mettait l'accent sur la nécessité de prendre en considération le meilleur intérêt de l'enfant tel qu'il est également établi à la Convention des Nations Unies relative aux droits de l'enfant. Le Groupe de travail veut souligner l'importance de ce principe également dans le contexte des Services des Réseaux Sociaux.»

13. **Lignes directrices de l'ITU pour les Décideurs** #5, 6 et 7: «*5. Considérer de prendre des mesures additionnelles pour interrompre ou réduire le trafic dans le CAM, par exemple, établir un service d'assistance téléphonique et développer des mesures qui bloquent l'accès à des sites web et des Forums de discussion d'Usenet connus pour contenir ou faire de la publicité de la disponibilité du CAM. 6. Assurer l'établissement d'un mécanisme et sa promotion largement afin de fournir un moyen de compréhension facile pour signaler le contenu illégal trouvé sur l'Internet, par exemple, un service d'assistance téléphonique qui ait la capacité de répondre rapidement et d'enlever or de rendre inaccessible le matériel illégal. 7. Assurer l'existence de processus nationaux qui garantissent que tout CAM trouvé dans un pays soit canalisé vers une ressource centralisée, nationale. Un exemple est le Centre National de Gestion du Matériel d'Abus des Enfants.»*

générés dans les réseaux sociaux numériques sont très dispersés et ils ne sont pas pleinement constatés.

16. Promouvoir des actions de sensibilisation et de diffusion des informations à travers les médias et les réseaux sociaux, parmi d'autres, car ceux-ci constituent un véhicule effectif pour encourager l'utilisation responsable et sûre des outils de la Société de l'information et de la connaissance.[14]

17. Promouvoir l'engagement et la participation des associations publiques et privées, ainsi que des réseaux nationaux de centres d'accès à l'Internet (là ou il y en a) afin d'assurer leur participation à la protection et aux campagnes d'alerte sur les potentialités et les risques de l'Internet et des réseaux sociaux numériques.

18. Stimuler la génération de connaissances spécialisées dans le but d'élaborer des politiques publiques adéquates. Notamment, en ce qui concerne les comportements en ligne des enfants et des adolescents, il est conseillé de faire des recherches sur les rôles qu'ils jouent dans la réception, la production, le stockage et la reproduction des contenus illégaux, les mesures de protection qu'ils développent, les motivations individuelles et collectives de ces comportements, ainsi que les dangers réels qu'ils trouvent dans la Société de l'information et de la connaissance.

RECOMMANDATIONS POUR L'INDUSTRIE

Les entreprises qui fournissent les services d'accès à Internet, qui développent les applications ou les réseaux sociaux numériques, doivent s'engager fermement en matière de protection des renseignements personnels et de la vie privée –notamment des enfants et des adolescents–, s'engager à coopérer avec les systèmes de justice nationaux, à développer des campagnes de prévention et de renforcement des capacités, parmi d'autres instruments, à travers des engagements ou des codes de conduite qui doivent comprendre :

19. L'interdiction de collecter, traiter, diffuser, publier ou transmettre à des tiers des renseignements personnels sans le consentement explicite de la personne concernée. Il faut restreindre l'utilisation de l'information recueillie dans un but différent de celui qui a motivé son traitement et, en particulier, de la création de profils de comportement.[15]

Dans le cas des enfants il faudra considérer l'interdiction du traitement des renseignements personnels. Dans le cas des adolescents il faudra prendre

14. **Liste de contrôle** #2 des **Lignes directrices de l'ITU pour les Décideurs** : «Il faudrait également considérer d'assurer l'aide des médias dans la promotion de messages et de campagnes de sensibilisation.»

15. **Opinion 5:** 3.4. Les renseignements personnels sensibles ne pourront être publiés sur l'Internet qu'avec le consentement explicite de la personne concernée ou si la personne concernée a divulgué manifestement ces renseignements elle-même.

en considération les mécanismes de contrôle des parents conformément à la législation de chaque pays, qui doivent être clairement communiqués.

20. La protection de la vie privée devrait être la caractéristique générale et, par défaut, dans tous les réseaux sociaux numériques, des bases de données et des systèmes de communication, etc. Les changements à effectuer dans le degré de confidentialité du profil de l'utilisateur doivent être simples et gratuits.

21. Les règles sur la confidentialité des pages web, des services, des applications, etc., devraient être explicites, simples et claires, exprimées dans un langage compréhensible pour les enfants et les adolescents.

Il faudra fournir des informations sur les buts et les fins de l'utilisation des renseignements personnels, ainsi que des transmissions effectuées à des tiers. Il faudra également indiquer les personnes responsables du traitement de l'information.

Il faut fournir aussi un lien vers les «paramètres de confidentialité» au moment de l'inscription, contenant une explication claire sur l'objet de ces paramètres.

Il faut rendre également accessible un avertissement sur le fait que le réseau social a présélectionné les paramètres, le cas échéant, et qu'ils peuvent être modifiés à tout moment selon les préférences des enfants et des adolescents.

Ce serait aussi souhaitable que les «paramètres par défaut» des contenus personnels soient modifiés afin qu'ils ne soient accessibles qu'aux amis et aux réseaux que l'utilisateur détermine.[16]

22. Tout réseau social numérique doit indiquer de façon explicite, dans la partie relative à la « publicité » contenue dans sa politique de confidentialité, les annonces publicitaires et informer de façon claire, notamment aux enfants et aux adolescents, que les renseignements personnels des profils des utilisateurs sont utilisés pour envoyer de la publicité selon chaque profil. Il faudra éviter la publicité non appropriée pour des enfants et des adolescents.[17]

23. Tout réseau social numérique doit indiquer de façon claire la raison pour laquelle il exige certains renseignements personnels et, en particulier, la date de naissance au moment de l'inscription et de la création du compte. Il faut donc expliquer que la date de naissance demandée a pour objet de pouvoir vérifier l'âge minimum pour pouvoir créer un compte sur le réseau social numérique.

---

16. Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt publique et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques, du 16 juillet 2009.*
17. *Id.*

Il faut également préciser de quelle façon seront utilisés ces renseignements personnels qu'il faut fournir de façon obligatoire.[18]

L'industrie devra mettre en pratique des mécanismes en vue de faire une vérification prouvée de l'âge des enfants et des adolescents pour la création d'un compte d'utilisateur et/ou pour accéder à un contenu déterminé.

24. Tout réseau social numérique, tout système de communication ou toute base de données devrait avoir des voies d'accès à l'information, de rectification et d'élimination des renseignements personnels pour des utilisateurs ou des non-utilisateurs, prenant en considération les limitations de la loi.[19]

Tout réseau social numérique doit élaborer une politique accessible aux utilisateurs en matière de conservation des informations en vertu de laquelle les renseignements personnels des utilisateurs qui ont désactivé leur compte soient complètement éliminés des serveurs du service après une période de temps raisonnable. En outre, il faudra éliminer les renseignements des non-utilisateurs considérant une limite raisonnable de conservation quand ils ont été invités à faire partie des réseaux. Les réseaux sociaux numériques ne doivent pas utiliser les renseignements des non-utilisateurs.

Les deux options qui permettent aux utilisateurs de désactiver et de supprimer les comptes doivent être complètement visibles ; les utilisateurs doivent pouvoir comprendre ce que chaque option suppose quant à la gestion des données contenues dans ces comptes de la part du service.[20]

Il faut informer les utilisateurs des obligations de confidentialité à l'égard des tiers ; cette politique doit être explicite, claire et visible.

25. Il faut empêcher l'indexage des utilisateurs des réseaux sociaux numériques par des navigateurs, sauf que l'utilisateur ait choisi cette fonction. L'indexage des renseignements des enfants doit être interdit sous toutes ses formes ; dans le cas des adolescents, ils doivent autoriser de façon expresse l'indexation de leurs renseignements minimums.

26. Tout réseau social numérique doit établir les mesures nécessaires pour limiter l'accès des tiers qui développent les diverses applications que le service offre (des jeux, des questionnaires, des annonces, etc.) aux renseignements personnels des utilisateurs s'ils ne sont pas nécessaires ou pertinents pour le fonctionnement de ces applications.

---

18. *Id*.

19. L'esprit de ce dernier paragraphe est de ne pas exclure —pour le temps nécessaire— la conservation des données des utilisateurs qui pourraient être nécessaires dans la recherche d'infractions.

20. Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt publique et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques, du 16 juillet 2009.*

Le réseau social doit assurer que les tiers qui développent des applications dans leurs plateformes pourront accéder aux renseignements personnels des utilisateurs uniquement avec leur consentement exprès. Le réseau social numérique doit s'assurer que les tiers développeurs demandent uniquement les renseignements indispensables, pertinents et non excessifs pour l'utilisation de cette application.

Il est important aussi de prendre les mesures nécessaires pour éviter toute communication de renseignements personnels des utilisateurs qui n'ont pas décidé de façon expresse par eux-mêmes d'installer une application.[21]

27. Ces recommandations s'appliquent au traitement des renseignements personnels aux réseaux sociaux numériques, même si leurs adresses légales se trouvent en dehors de l'Amérique Latine et les Caraïbes. Pour faciliter l'accès des utilisateurs à la justice, chaque entreprise fournisseuse de réseaux sociaux numériques doit élire un domicile ou un représentant légal dans les pays où ce réseau social est utilisé de façon significative ou à réquisitoire de l'État.

Les réseaux sociaux numériques devront créer un service efficace et efficient de support aux utilisateurs dans ces sujets dans les langues officielles utilisées dans le pays de l'utilisateur.

28. Les développeurs de pages web, de services, d'applications, de plateformes, etc., devront établir des filtres de sécurité comme un moyen complémentaire à l'éducation, la sensibilisation et la sanction.[22]

29 L'industrie doit établir des mesures techniques et opérationnelles pour garantir la sécurité de l'information, en particulier l'intégrité, la disponibilité et la confidentialité.

30. Pour l'éradication de la pornographie infantile sur l'Internet, l'industrie – dans un effort conjoint de tous les acteurs responsables– doit s'engager au minimum à:

30.1. Notifier les autorités compétentes de toute apparition de pornographie infantile dans des profils des utilisateurs de réseaux sociaux numériques afin de pouvoir instruire les enquêtes et les actions correspondantes;

30.2. Préserver toutes les données nécessaires pour l'enquête pendant un délai minimum de six mois ou remettre ces données aux autorités compétentes, moyennant une autorisation judiciaire;

---

21. Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt publique et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques, du 16 juillet 2009.*

22. **Lignes directrices de l'ITU pour les Décideurs** #13 : *«Considérer le rôle qui peuvent jouer les outils techniques comme des programmes de filtrage et des logiciels pour la sécurité de l'enfant en appuyant et en supplémentant des initiatives d'éducation et de sensibilisation.»*

30.3. Préserver les contenus publiés par les utilisateurs des réseaux sociaux pendant le même délai et remettre ces contenus aux autorités publiques moyennant une autorisation judiciaire;

30.4. Appliquer de façon intégrale les législations nationales par rapport aux crimes cybernétiques commis par les citoyens des pays latino-américains et des Caraïbes ou moyennant des connexions à l'Internet faites depuis les juridictions nationales respectives;

30.5. Reformuler le service d'aide aux utilisateurs pour donner une réponse dans un délai raisonnable à toutes les réclamations, faites par courrier électronique ou par courrier postal, des personnes lésées à cause de la création de communautés fausses au offensives;

30.6. Développer une technologie efficace de filtrage et de mise en pratique de modération humaine pour empêcher la publication de photographies et d'images de pornographie infantile sur le service des réseaux sociaux numériques;

30.7. Développer des outils à travers lesquels les lignes téléphoniques d'aide aux enfants et aux adolescents puissent acheminer les plaintes pour que les employés de l'entreprise analysent et retirent les contenus illégaux, qu'ils informent les autorités compétentes lorsqu'ils aient des indices de pornographie infantile, de racisme ou d'autres crimes de haine, et qu'ils préservent toutes les preuves;

30.8. Retirer les contenus illicites, soit moyennant une décision judiciaire, soit par mise en demeure d'une autorité publique compétente, tout en préservant les données nécessaires pour l'identification des auteurs de ces contenus;

30.9. Développer des outils de communication avec les autorités compétentes pour faciliter les démarches par rapport aux plaintes, la formulation des demandes de retrait et la préservation des données;

30.10. Notifier les utilisateurs nationaux de façon adéquate sur les principaux délits commis dans les réseaux sociaux numériques (pornographie infantile, crimes de haine, délits contre l'honneur, etc.);

30.11. Développer des campagnes d'éducation pour l'utilisation sûre et respectueuse des lois, de l'Internet et des réseaux sociaux numériques;

30.12. Financer la publication de brochures et leur distribution aux enfants et aux adolescents dans des écoles publiques, contenant des informations pour l'utilisation sûre de l'Internet et des réseaux sociaux;

30.13. Maintenir un lien, dans les sites des réseaux sociaux numériques, avec des sites pour dénoncer ou des lignes d'aide aux enfants et aux adolescents.

CONSIDÉRATIONS FINALES

31. Les recommandations indiquées pour les enfants et les adolescents comprennent d'autres personnes (majeures) qui, en raison de leur condition personnelle, se trouvent dans une position de vulnérabilité.

Sont considérés des groupes vulnérables tous ceux en rapport aux données sensibles (selon chacune des législations nationales) qui comprennent généralement des travailleurs, des dissidents, des personnes handicapées et leurs familles, des immigrants et des émigrants, etc.

32. Tous les acteurs concernés sont priés de discuter et d'interpréter ces recommandations. Il faut également chercher un dialogue constant à ce sujet prenant en considération le présent document. De façon spéciale on fait appel à l'exécution des obligations des États et à la responsabilité sociale des entreprises pour trouver les meilleures formes de mettre en application le présent document.

A Montevideo, le 28 juillet 2009

Recommandations adoptées au *Séminaire Droits, Adolescents et Réseaux Sociaux sur l'Internet* (avec la participation de Belén Albornoz, Florencia Barindeli, Chantal Bernier, Miguel Cillero, José Clastornik, Rosario Duaso, Carlos G. Gregorio, Esther Mitjans, Federico Monteverde, Erick Iriarte, Thiago Tavares Nunes de Oliveira, Lina Ornelas, Leila Regina Paiva de Souza, Ricardo Pérez Manrique, Nelson Remolina, Farith Simon et María José Viega) tenu à Montevideo le 27 et le 28 juillet 2009.