COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD-BUR(2011) 05 prov fr
21 avril 2011

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL
(T-PD-BUR)

Projet d'avis du Bureau du T-PD sur les projets de textes préparés par le Comité d'experts sur les nouveaux médias (MC-NM) au sujet des services de réseaux sociaux

Document préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

Introduction

1. Le Bureau du Comité Consultatif de la Convention (ETS n°108) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) tient en premier lieu à saluer le travail du Comité d'Experts sur les nouveaux médias (MC-NM).

2. Le Bureau du T-PD a été saisi d'une demande d'opinion des deux projets de textes préparés par le MC-NM sur la question des services de réseaux sociaux, un projet de Recommandation d'une part (document MC-NM (2010)3) et un projet de lignes directrices destinées aux fournisseurs d'autre part (document MC-NM (2010)8).

3. Après avoir procédé à un premier échange de vues sur ces projets lors de sa 23ème réunion (22-24 mars 2010), le Bureau a appelé ses membres à faire part au Secrétariat de commentaires écrits sur les textes, en vue de la préparation de son avis.

4. Il convient de souligner que le présent avis émane du Bureau du T-PD et qu'une consultation du T-PD dans son ensemble paraît opportune au vu de l'importance des problématiques concernées. Il est envisagé de procéder à cette consultation des membres du T-PD par consultation écrite, sur la base du présent avis et des projets de texte et de transmettre la position du T-PD au Comité Directeur sur les médias et les nouveaux services de communication (CDMC) en vue de sa réunion plénière des 14-17 juin 2011.

Structure

5. Le Bureau du T-PD tient en premier lieu à souligner que l'articulation entre les deux projets de texte (recommandation et lignes directrices) n'est pas toujours aisée, notamment en raison du fait que la recommandation fait elle-même référence à des lignes directrices (son annexe).

6. Bien qu'il soit précisé dans les lignes directrices destinées aux fournisseurs qu'elles doivent être « lues et comprises dans le cadre […du projet de] recommandation » il semble important de prévoir qu'un ensemble cohérent et exhaustif de principes soit également proposé aux fournisseurs. Les lignes directrices destinées aux fournisseurs ne font par exemple pas référence à l'indexation de données par des moteurs de recherche externes alors que les mesures permettant à l'utilisateur de manifester son consentement libre, spécifique et éclairé à cette indexation ; mesures qui doivent être systématiquement prévues par défaut, concernent au premier plan les fournisseurs. Ce point pourrait notamment être ajouté après celui relatif à la limitation par défaut de l'accès des données aux « amis[1] » sélectionnés par l'utilisateur.

Références

7. Le Bureau du T-PD attire l'attention du MC-NM sur les textes adoptés en la matière aux niveaux européen et international, auxquels il conviendrait de faire référence, pour le moins dans l'exposé des motifs de la recommandation, à commencer par la Convention 108.

8. Il s'agit en particulier de l'avis 5/2009 sur les réseaux sociaux en ligne adopté le 12 juin 2009 par le Groupe de Travail « Article 29 » sur la protection des données, de la Résolution sur la protection de la vie privée dans les services de réseaux sociaux adoptée le 17 octobre 2008 à Strasbourg par la 30ème Conférence internationale annuelle des Commissaires à la protection des données et à la vie privée et du rapport en la matière adopté à Rome les 3-4 mars 2008 par le Groupe International de travail sur la protection des données dans les télécommunications (IWGDPT), dit le « mémorandum de Rome ».

Principes de protection des données

9. D'une façon générale, il convient de faire référence à la « finalité » du traitement plutôt qu'à l' « objectif ». Il conviendrait par ailleurs d'illustrer ce que sont des finalités légitimes ou illégitimes.

[1] Cette notion d'amis parait inappropriée aux réseaux sociaux basés sur les relations professionnelles.

10. S'agissant des droits des intéressés, le Bureau du T-PD souligne en premier lieu la nécessité d'une information générale, claire et compréhensible des utilisateurs des services sociaux, c'est-à-dire de tous les utilisateurs, avec le cas échéant un langage adapté à la population cible. Cette information devrait être disponible dans la langue officielle du pays de résidence des différents groupes d'utilisateurs. L'information doit permettre d'attirer l'attention des utilisateurs sur les dangers de la publicisation de toute donnée, ainsi que sur les possibilités qui leur sont offertes de limiter les accès afin de préserver une sphère privée. Cette information doit être complète et porter sur la durée de conservation des données, les modalités d'exercice des droits d'accès et d'opposition, les conditions d'indexation des données par des moteurs de recherche. Enfin, cette information doit rappeler la législation applicable en la matière.

11. Il convient par ailleurs de souligner que les droits que les utilisateurs exercent sur leurs données personnelles ne se limitent pas à la seule suppression des données (« profil » – notion à définir) et que les fournisseurs doivent rendre l'exercice des différentes fonctionnalités simple. La notion de « portabilité » des données et ce qu'elle implique devrait apparaître dans les projets. Les interfaces à disposition des utilisateurs doivent être simples d'utilisation et permettre aux personnes concernées de bien saisir les implications de telle ou telle action sur leurs données personnelles (par exemple qu'en utilisant telle application, c'est la totalité du répertoire de mes contacts qui sera utilisée pour des notifications directes de ces contacts, ce qui devrait impérativement nécessiter un consentement préalable).

12. S'agissant de régimes de protection renforcés, le Bureau du T-PD note que d'autres catégories vulnérables de personnes que celle des enfants peuvent avoir besoin de tels régimes.

13. Le Bureau du T-PD souligne l'impératif de prudence dans l'utilisation des mécanismes de vérifications de l'âge et invite à recommander de développer ces systèmes de vérification en conformité avec les droits de l'homme.

14. S'agissant du traitement des données par des tiers et de l'obligation pour le fournisseur « de rechercher le consentement informé des utilisateurs avant que leurs données ne soient traitées» (supprimer 'à leur insu' qui ne correspond pas à l'effet du consentement donné préalablement), il devrait être précisé que la décision de l'utilisateur (refus ou consentement) ne peut avoir de conséquence sur la possibilité de continuer à bénéficier du service. L'on peut par ailleurs se demander si ce consentement doit être obtenu avant que les données ne soient 'traitées' ou plutôt transmises au tiers, et enfin, s'il est nécessaire de préciser qu'il s'agit d'un tiers 'proposant des applications'. Le Bureau du T-PD attire à cet égard l'attention du MC-NM sur la Recommandation (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, qui constate en son préambule que le traitement de données aux fins de profilage peut concerner des données provenant de réseaux sociaux.

15. L'indexation des données personnelles publiées par les moteurs de recherche devrait par principe être interdite et n'être rendue possible qu'après avoir obtenu le consentement libre, spécifique et éclairé de la personne concernée.

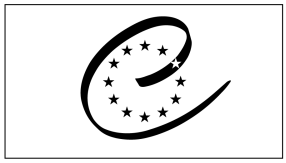
16. Les fournisseurs devraient respecter le principe de minimisation : la limitation du traitement aux seules données strictement nécessaires aux finalités consenties, et pour une durée aussi courte que possible.

17. L'appel à l'utilisation de « mesures de sécurité les plus récentes » (ne serait-ce pas plutôt des mesures de sécurité appropriées ?) pour protéger les données contre un accès illicite de la part de tiers est a saluer.

18. Au vu de l'actualité récente, ne serait-il pas opportun de rappeler les conditions dans lesquelles des données personnelles détenues par les fournisseurs peuvent être utilisées par les autorités chargées de l'application de la loi (police), et les mécanismes de protection qui doivent encadrer un tel usage (Recommandation N° R (87) 15 visant à réglementer l 'utilisation de données à caractère personnel dans le secteur de la police).

19. Enfin, il devrait être prévu que les autorités de protection des données soient appelées à contribuer à la mise en place des mécanismes de corégulation ou d'autorégulation (notamment dans le cadre de l'élaboration de codes de conduite, de cadres de référence, etc.).

Annexe 1 : Projet de recommandation sur les mesures de protection et de promotion des droits de l'homme dans le cadre des services de réseaux sociaux [MC-NM(2010)003_fr]



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 mars 2010

MC-NM(2010)003_fr
English
Pdf

COMITÉ D'EXPERTS SUR LES NOUVEAUX MÉDIAS

(MC-NM)

_____

2e réunion
25 – 26 mars 2010
Agora
Salle G 05

_____

Projet de recommandation sur les mesures de protection et de promotion des droits de l'homme dans le cadre des services de réseaux sociaux

_____

1. Les services de réseaux sociaux jouent un rôle de plus en plus important dans la vie quotidienne. Ils constituent un outil d'expression mais servent également à communiquer entre individus ou à une communication de masse. En raison de ces caractéristiques complexes, ils offrent de grandes possibilités de promouvoir l'exercice et la jouissance des droits de l'homme et des libertés fondamentales, notamment la liberté d'exprimer, de créer et d'échanger des contenus et des communications.

2. Etant donné leur rôle de plus en plus important, les services de réseaux sociaux et les autres services de médias sociaux offrent aussi de grandes possibilités de promouvoir le droit de l'individu à participer à la vie politique, sociale et culturelle. Compte tenu de la Recommandation (2007)16 du Comité des Ministres sur des mesures visant à promouvoir la valeur de service public de l'internet, qui indique qu'internet et les autres services utilisant les TIC présentent un grand intérêt en matière de service public car ils servent à promouvoir l'exercice et la jouissance des droits de l'homme et des libertés fondamentales pour tous leurs utilisateurs, des moyens plus importants pourraient être consacrés à l'étude de la manière dont les services de réseaux sociaux et autres médias sociaux pourraient aider à favoriser la participation (notamment des groupes marginalisés de la société) et contribuer au renforcement de la démocratie et de la cohésion sociale.

3. Le droit à la liberté d'expression et d'information, ainsi que le droit au respect de la vie privée et de la dignité humaine peuvent aussi être menacés sur les sites des réseaux sociaux. Ces menaces sont dues, par exemple, à l'absence de procédure équitable avant l'exclusion des utilisateurs, à la protection insuffisante des mineurs contre les comportements préjudiciables d'autres personnes, à la violation des droits d'autrui et à l'absence de transparence concernant les objectifs dans lesquels sont collectées et traitées les données à caractère personnel.

4. Les utilisateurs des services de réseaux sociaux doivent respecter les droits et des libertés d'autrui. L'éducation aux médias est particulièrement importante dans le domaine des services de réseaux sociaux pour faire prendre conscience aux utilisateurs de leurs droits lorsqu'ils utilisent ces outils. Les compétences médiatiques de base doivent aussi couvrir les valeurs des droits de l'homme et les comportements nécessaires au respect des droits et libertés d'autrui.

5. Un certain nombre de mécanismes de corégulation et d'autorégulation ont déjà été mis en place dans des Etats membres du Conseil de l'Europe. Il est important que ces mécanismes respectent le principe de la procédure équitable et que tout mécanisme de réparation soit indépendant, transparent, efficace et qu'il rende des comptes.

6. Le Comité des Ministres recommande aux Etats membres d'élaborer et de promouvoir en coopération avec les acteurs du secteur privé et la société civile des stratégies cohérentes visant à protéger et à promouvoir le respect des droits de l'homme dans le cadre des services de réseaux sociaux, notamment :

- en vérifiant que les utilisateurs sont conscients des menaces éventuelles que les services de réseaux sociaux font peser sur leurs droits (en particulier leur liberté d'expression et d'information et leur droit au respect de la vie privée et à la protection des données personnelles) ainsi que des moyens d'éviter de nuire aux droits d'autrui lorsqu'ils utilisent ces services ;

- en protégeant les utilisateurs des services de réseaux sociaux contre les préjudices causés par d'autres utilisateurs, tout en garantissant le droit de tous à la liberté d'expression et à l'accès à l'information ;

- en encourageant la transparence concernant les différentes sortes de données personnelles collectées et les objectifs légitimes pour lesquels elles sont traitées, y compris un traitement ultérieur par des tiers ;

- en empêchant le traitement illégitime des données à caractère personnel ;

- en encourageant les fournisseurs de services de réseaux sociaux à mettre en place des mécanismes de corégulation ou d'autorégulation efficaces, transparents, indépendants et responsables et qui accordent aux individus un droit de recours contre leurs décisions ;

- en portant les présentes lignes directrices à l'attention de tous les partenaires pertinents des secteurs privé et public, notamment les fournisseurs de réseaux sociaux et la société civile ;

- en prenant des mesures en ce qui concerne les services de réseaux sociaux conformément aux lignes directrices figurant en annexe à la présente recommandation.

Annexe – Lignes directrices

I. La transparence concernant la liberté d'expression et l'accès à l'information

1. Les services de réseaux sociaux permettent de recevoir et de diffuser des informations. Les utilisateurs peuvent choisir individuellement les destinataires de ces informations, mais le plus souvent ces destinataires sont un ensemble dynamique de personnes, parfois même une « masse » d'inconnus (tous les membres du réseau social). Lorsque les profils des utilisateurs (ou certaines parties de ces profils) sont indexés par des moteurs de recherche, il y a un accès potentiellement illimité à certaines parties ou à la totalité des informations publiées sur ces profils.

2. Il est important que les participants aient confiance lorsqu'ils diffusent des informations et sachent si les informations qu'ils diffusent ont un caractère public ou privé. En particulier, les enfants et les adolescents ont besoin de conseils pour pouvoir gérer leur profil et comprendre l'impact que peut avoir une expression privée et (semi) publique, afin d'éviter de se mettre en danger et de nuire à autrui. En coopération avec le secteur privé et la société civile, les Etats membres devraient veiller à ce que le droit des utilisateurs à la liberté d'expression soit respecté, notamment :

- en informant clairement les utilisateurs de la différence entre une communication privée et une communication publique et des conséquences éventuelles d'un accès illimité (dans le temps et géographiquement) à leur profil et à leurs communications ;

- en fournissant des informations sur les conditions essentielles de participation aux services de réseaux sociaux sous une forme et dans une langue adaptées aux groupes cibles des sites de réseaux sociaux, et facilement compréhensible par ces groupes ;

- en encourageant les initiatives de sensibilisation destinées aux parents et aux enseignants en vue de compléter les informations fournies par les services de réseaux sociaux.

II. Protection appropriée des enfants contre les contenus et les comportements préjudiciables

3. La liberté d'expression comprend la liberté de diffuser et de recevoir des contenus choquants,, troublants et insultants et/ou des contenus ne convenant pas à certains groupes d'âge. Dans certains cas cependant, la dignité humaine et l'obligation de respecter et de protéger les droits des groupes vulnérables peuvent l'emporter sur ce droit à la liberté d'expression.

4. Les réseaux de services sociaux jouent un rôle de plus en plus important dans la vie des mineurs, en contribuant au développement de leur personnalité et de leur identité ainsi qu'à leur participation au débat (semi) public. De la même façon, il faut aussi protéger les mineurs vulnérables du fait de leur âge.

5. [Des mécanismes de vérification de l'âge peuvent constituer un moyen de protéger les enfants de contenus potentiellement préjudiciables. Toutefois, il n'existe pas de solution technique unique pour la vérification de l'âge en ligne qui ne porte pas atteinte à d'autres droits et/ou n'encourage pas la falsification de l'âge, entraînant ainsi pour les mineurs concernés des risques supérieurs au bénéfice attendu]. En collaboration avec le secteur privé et la société civile, les Etats membres doivent veiller à la sécurité des utilisateurs et protéger leur dignité, tout en respectant les garanties de procédure et le droit à la liberté d'expression et à l'accès à l'information, notamment :

- en indiquant aux utilisateurs quels sont les contenus considérés « illicites » selon les dispositions légales et quels sont les contenus ou comportements considérés « inappropriés » selon les conditions générales des sites des réseaux sociaux ;

- en encourageant les forces de l'ordre et les sites de réseaux sociaux à mettre en place une base de coopération transparente prévoyant des mesures ayant fait leurs preuves ou des permanences téléphoniques (hotlines) ;

- en veillant à ce que les utilisateurs aient accès à un mécanisme facile d'emploi pour signaler aux fournisseurs de sites les contenus ou les comportements inappropriés et illicites d'autres utilisateurs ;

- en adoptant d'autres mesures spécifiques visant à prévenir le harcèlement et la sollicitation en ligne, tels que l'étiquetage des contenus et la classification du contenu par tranches d'âge ; [toutefois, il convient de traiter avec prudence l'offre d'accès en fonction de l'âge puisqu'elle dépend d'informations fournies par les mineurs eux-mêmes] ;

- en veillant à ce que toute décision visant à bloquer un contenu soit prise conformément à la Recommandation (2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, et à ses lignes directrices ;

- en garantissant notamment que des mesures générales de blocage ou de filtrage au niveau national ne seront introduites par l'Etat que si les conditions de l'article 10, paragraphe 2 de la Convention européenne des droits de l'homme sont remplies et si ces mesures évitent de bloquer totalement les contenus injurieux ou préjudiciables pour les utilisateurs qui ne font pas partie des groupes protégés par un filtre. [Sinon, le fait d'encourager les services de réseaux sociaux à offrir des mécanismes volontaires et adaptés de filtrage individuel peut suffire à protéger ces groupes.]

III. Garantir aux utilisateurs le contrôle de leurs données

5. Les réseaux sociaux traitent d'énormes quantités de données personnelles. Ils doivent absolument appliquer les mesures de sécurité les plus récentes pour protéger ces données contre un accès illicite de la part de tiers. L'accès des tiers peut également être obtenu par le biais d'applications proposées par ces tiers. Les services de réseaux sociaux ne doivent pas traiter des données personnelles au-delà des finalités légitimes et spécifiées pour lesquelles ils les ont collectées et doivent rechercher le consentement informé des utilisateurs avant que leurs données ne soient traitées à leur insu par des tiers proposant des applications.

6. La configuration proposée par défaut aux utilisateurs doit être un accès limité aux amis qu'ils sélectionnent eux-mêmes. Les utilisateurs doivent pouvoir prendre une décision informée pour autoriser l'accès d'un public plus vaste à leurs données. Le service de réseau social doit offrir des possibilités adéquates et bien conçues d'accepter (« opt in ») un accès plus large. Si un utilisateur souhaite autoriser tous les utilisateurs du réseau ou même de l'internet à accéder à ses données en permettant l'indexage de son profil par des moteurs de recherche externes, il doit savoir clairement comment il peut restreindre de nouveau cet accès, y compris en supprimant ses données des archives et des fichiers temporaires des moteurs de recherche, et doit pouvoir accéder facilement aux outils appropriés.

7. Les utilisateurs doivent être informés des risques possibles concernant le respect de leur vie privée. Ces informations doivent être fournies non seulement dans les conditions générales des sites de réseaux sociaux mais aussi chaque fois qu'un tel risque peut survenir, par exemple lorsque les utilisateurs mettent des informations sur leur profil à la disposition de nouveaux (groupes d') utilisateurs ou lorsqu'ils installent une application proposée par un tiers. En particulier, les enfants et les adolescents ont besoin de conseils spéciaux pour pouvoir gérer leur profil et comprendre les risques pour le respect de leur vie privée d'une modification de leurs paramètres pour adopter un profil plus public.

8. L'utilisation de profils avec pseudonyme représente à la fois des chances et des risques en matière de droits de l'homme. Dans sa déclaration sur la liberté de la communication sur l'internet (adoptée le 28 mai 2003), le Comité des Ministres soulignait 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 ». Il convient d'encourager cette pratique tant dans la perspective de la libre expression des informations et des idées que dans la perspective du droit au respect de la vie privée. Elle doit, cependant, aussi s'accompagner d'un système de contrôle efficace des comportements inappropriés, comme des mécanismes de réclamation et de signalement, de modération, etc.

9. En collaboration avec le secteur privé et la société civile, les Etats membres devraient veiller à la protection du droit au respect de la vie privée, notamment :

- en mettant en œuvre les règles applicables sur le respect de la vie privée, notamment celles selon lesquelles les services de réseaux sociaux limitent par défaut l'accès aux amis sélectionnés par l'utilisateur, appliquent les mesures de sécurité les plus récentes et s'appuient sur des motifs

légitimes pour le traitement des données personnelles à des fins spécifiques, y compris le traitement ultérieur par des tiers et l'utilisation à des fins de ciblage comportemental ;

- en veillant à l'information transparente des utilisateurs concernant la gestion de leurs données personnelles sous une forme et dans une langue adaptées aux groupes cibles des services de réseaux sociaux ;

- en veillant à ce que les utilisateurs soient informés de la nécessité d'obtenir le consentement préalable d'autres personnes avant de publier leurs données personnelles, y compris les données audio et vidéo, dans les cas où ils ont élargi l'accès à leurs propres données au-delà du cercle restreint des amis qu'ils ont eux-mêmes sélectionnés ;

- en garantissant aux utilisateurs qu'ils peuvent complètement supprimer d'un service de réseau social leur profil et toutes les données stockées qui les concernent ou qu'ils ont envoyées [ce qui inclut les outils dont disposent les parents pour gérer les données concernant leurs enfants] ;

- en permettant l'utilisation de pseudonymes pour les profils.

V. Autorégulation et corégulation

1. Il existe en Europe plusieurs exemples d'initiatives de fournisseurs de services de réseaux sociaux en matière d'autorégulation. Ces initiatives méritent d'être saluées. Il est important de rappeler que toute autorégulation ou corégulation, en tant que forme d'interférence, devrait être transparente, indépendante, responsable et efficace. Les Etats membres devraient :
- assurer que tous les dispositifs d'autorégulation correspondent aux exigences minimum de la Convention européenne des droits de l'homme, et en particulier le droit à une procédure équitable. Les mécanismes de réclamation doivent être transparents, efficaces, indépendants et responsables.

Annexe 2 : Proposition pour un projet de lignes directrices à l'intention des fournisseurs de réseaux sociaux [MC-NM(2010)008_fr]

Strasbourg, 5 octobre 2010

MC-NM(2010)008_fr
English
Pdf

COMITÉ D'EXPERTS SUR LES NOUVEAUX MÉDIAS
(MC-NM)

_____

2ème réunion
25 – 26 mars 2010
Bâtiment Agora
Salle G 05

____

Proposition pour un projet de LIGNES DIRECTRICES A L'INTENTION DES FOURNISSEURS DE RÉSEAUX SOCIAUX

Les services de réseaux sociaux fournissent une plate-forme très importante à la fois pour recevoir et pour transmettre des informations. Par conséquent, ils représentent un outil important tant pour le droit fondamental à la liberté d'expression, que pour la participation à la vie sociale, culturelle, économique [et même dans certains cas, politique].

Il est important que les utilisateurs des services de réseaux sociaux se sentent confiants quant à l'utilisation de ces outils. Ils doivent avoir la certitude que leur droit à la vie privée sera protégé lorsqu'ils utilisent des services de réseaux sociaux et que leurs données personnelles ne seront pas employées abusivement. Ils doivent aussi savoir à quel moment l'information qu'ils diffusent en ligne ne relève plus la correspondance privée, mais est devenue accessible à un large public.

Il est tout aussi important de rappeler que l'exercice de la liberté d'expression comporte des devoirs et des responsabilités, notamment en ce qui concerne la protection de la santé, de l'éthique et des droits de tous les utilisateurs. Les fournisseurs de réseaux sociaux sont encouragés à veiller à ce que les utilisateurs soient protégés contre les contenus nuisibles ou des actions telles que le harclèlement en ligne.

Les fournisseurs de réseaux sociaux doivent promouvoir et faciliter le bien-être des utilisateurs tout en respectant les droits fondamentaux, en particulier le droit à la liberté d'expression et le droit à la vie privée et au secret de la correspondance.

Par conséquent, les fournisseurs de réseaux sociaux sont invités à prendre note, discuter et faire le maximum d'efforts pour se conformer aux lignes directrices suivantes (ci-dessous). Ces lignes directrices doivent être lues et comprises dans le cadre des documents pertinents du Conseil de l'Europe, en particulier le [Projet] de Recommandation sur des mesures pour protéger et promouvoir le respect des droits de l'homme en matière de services de réseaux sociaux [CMRec ...].

- Informer clairement les utilisateurs sur les conditions d'utilisation sous une forme et un langage qui est approprié et facilement compréhensible par les groupes cibles du site de réseaux sociaux (par exemple, par le biais de courtes vidéos ou d'informations en «langage clair»).

- Informer les utilisateurs, en particulier sur la différence entre communication privée et publique et les éventuelles conséquences d'un accès illimité (dans le temps et géographiquement) à leur profil et communication.

- Si possible, offrir ou contribuer à des initiatives de sensibilisation pour les utilisateurs, les parents et les enseignants sur l'utilisation sans danger des services de réseaux sociaux.

- Informer clairement l'utilisateur sur les contenus considérés comme «illégaux» conformément aux dispositions juridiques et sur les contenus ou comportements considérés comme «inappropriés» conformément aux expressions et conditions générales du site de réseau social.

- Garantir que les utilisateurs ont accès à un mécanisme facile d'utilisation pour signaler des contenus inappropriés et illégaux ou le comportement d'autres utilisateurs aux fournisseurs du site.

- Adopter d'autres mesures spécifiques visant à prévenir le harcèlement et la sollicitation en ligne, telles que l'étiquetage des contenus et la classification du contenu par tranches d'âge ; [toutefois, il convient de traiter avec prudence l'offre d'accès en fonction de l'âge puisqu'elle dépend d'informations fournies par les mineurs eux-mêmes].

- Mettre en place une base de coopération transparente prévoyant des mesures ayant fait leurs preuves ou des permanences téléphoniques (hotlines).

- Veiller à ce que toute les décisions visant à bloquer des contenus soit prise conformément à la Recommandation (2008)6 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet et de ses lignes directrices.

- De garantir, en particulier, que les mécanismes d'autorégulation mis en place pour protéger les utilisateurs contre les contenus illicites et préjudiciables soient efficaces, transparents,

indépendants et puissent rendre des comptes et qui accordent aux individus un droit de recours contre leurs décisions de bloquer du contenu.

- Respecter les règlements applicables à la vie privée, en particulier limiter par défaut l'accès aux amis sélectionnés par l'utilisateur, appliquer les mesures de sécurité les plus récentes et s'appuyer sur des motifs légitimes pour le traitement des données à caractère personnel à des fins spécifiques, y compris le traitement ultérieur par des tiers et l'utilisation à des fins de ciblage comportemental.

- Veuiller à une information transparente des utilisateurs concernant la gestion de leurs données personnelles, sous une forme et une langue adaptées aux groupes cibles des services de réseaux sociaux.

- Veiller à ce que les utilisateurs soient informés de la nécessité d'obtenir le consentement préalable d'autres personnes avant de publier leurs données personnelles, y compris les données audio et vidéo, dans les cas où ils ont élargi l'accès à leurs propres données au-delà du cercle restreint des amis qu'ils ont eux-mêmes sélectionnés.

- Garantir aux utilisateurs qu'ils peuvent complètement supprimer d'un réseau social leur profil et toutes les données stockées qui les concernent ou qu'ils ont envoyées [ce qui inclut des outils dont disposent les parents pour gérer les données concernant leurs enfants].

- Permettre l'utilisation de pseudonymes pour les profils.