COUNCIL OF EUROPE CONSEIL DE L'EUROPE
Committee of Ministers
Comité des Ministres

Recommandation CM/Rec(2012)4
du Comité des Ministres aux Etats membres
sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux

(adoptée par le Comité des Ministres le 4 avril 2012,
lors de la 1139e réunion des Délégués des Ministres)

Les réseaux sociaux comme moyens de promotion des droits de l'homme et catalyseurs en faveur de la démocratie

1. Les services de réseaux sociaux jouent un rôle considérable dans la vie quotidienne d'un nombre croissant de gens. Ils sont un outil d'expression et de communication entre individus, mais aussi un outil de communication directe de masse ou de communication de masse de groupe. Cette complexité offre aux opérateurs de services de réseaux sociaux ou de plateformes 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 idées, et la liberté de réunion. Les services de réseaux sociaux peuvent aider le grand public à recevoir et à communiquer des informations.

2. L'importance croissante du rôle des services de réseaux sociaux et des autres services de médias sociaux offre aussi de grandes opportunités pour renforcer la possibilité pour les individus de participer à la vie politique, sociale et culturelle. Le Comité des Ministres a reconnu la valeur de service public d'internet en ce qu'il contribue, avec d'autres technologies de l'information et de la communication (TIC), à promouvoir l'exercice et la jouissance des droits de l'homme et des libertés fondamentales de tous ses utilisateurs. Ces réseaux sociaux, qui font partie intégrante de la valeur de service public d'internet, peuvent contribuer à la démocratie et à la cohésion sociale.

Les droits de l'homme peuvent être menacés sur les réseaux sociaux

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 réseaux sociaux, qui peuvent également contenir des pratiques discriminatoires. Ces menaces peuvent notamment découler de l'absence de garanties juridiques et procédurales, dans des procédés qui peuvent conduire à l'exclusion d'un utilisateur ; d'une protection inadaptée des enfants et des jeunes contre des contenus ou comportements susceptibles de leur être préjudiciables ; d'un manque de respect pour les droits d'autrui ; de l'absence d'une configuration par défaut qui respecte la vie privée ; d'un manque de transparence des finalités pour lesquelles les données à caractère personnel sont collectées et traitées.

4. Les utilisateurs des services de réseaux sociaux devraient respecter les droits et les 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, ainsi que pour leur permettre d'acquérir ou de renforcer les valeurs des droits de l'homme et de développer les comportements indispensables au respect des droits et libertés d'autrui.

Les fournisseurs de réseaux sociaux devraient respecter les droits de l'homme et la prééminence du droit

5. Quelques Etats membres du Conseil de l'Europe ont déjà mis en place des mécanismes d'autorégulation et de corégulation en liaison avec les normes d'utilisation des réseaux sociaux. Il est important que ces mécanismes respectent les garanties procédurales, conformément au droit à être entendu et au droit de contester ou faire appel des décisions rendues, y compris, lorsque cela s'avère nécessaire, au droit à un procès équitable, dans un délai raisonnable, à commencer par la présomption d'innocence.

6. En vertu du libellé de l'article 15.*b* du Statut du Conseil de l'Europe, le Comité des Ministres recommande aux Etats membres d'élaborer et de promouvoir, en concertation 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, conformément à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (STE n° 5, ci-après « Convention européenne des droits de l'homme ») et, notamment, l'article 8 (Droit au respect de la vie privée et familiale), l'article 10 (Liberté d'expression) et l'article 11 (Liberté de réunion et d'association), et à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), tout particulièrement en s'engageant avec les fournisseurs de réseaux sociaux à mener les actions suivantes :

– offrir un environnement qui permette aux utilisateurs de réseaux sociaux de continuer à exercer leurs droits et libertés ;

– sensibiliser les utilisateurs, par un langage clair et compréhensible, aux éventuelles atteintes à leurs droits fondamentaux et aux moyens d'éviter d'avoir un impact négatif sur les droits d'autrui lorsqu'ils utilisent ces services ;

– protéger les utilisateurs contre tout préjudice, sans pour autant limiter la liberté d'expression et l'accès à l'information ;

– renforcer la transparence quant au traitement des données et s'abstenir de tout traitement illégitime des données à caractère personnel ;

– mettre, le cas échéant, en place des mécanismes d'autorégulation et de corégulation, afin de contribuer au respect des objectifs énoncés dans l'annexe à la présente recommandation ;

– assurer l'accessibilité à leurs services pour les personnes handicapées, ce qui permettra d'améliorer l'intégration de ces personnes et leur pleine participation à la société.

7. Les Etats membres devraient :

– prendre des mesures conformes aux objectifs énoncés à l'annexe à la présente recommandation ;

– porter la présente recommandation et son annexe à l'attention de tous les partenaires pertinents des secteurs public et privé, notamment les fournisseurs de réseaux sociaux et la société civile.

Annexe à la Recommandation CM/Rec(2012)4

I. Informations et mesures essentielles pour aider les individus dans leur utilisation des réseaux sociaux

Contexte et défis

1. Les services de réseaux sociaux permettent à la fois 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 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 utilisateurs aient confiance en ce que les informations qu'ils partagent soient traitées de manière appropriée. Ils devraient savoir si ces informations ont un caractère public ou privé et avoir conscience des conséquences résultant du choix de rendre une information publique. Les enfants et les adolescents plus particulièrement, ainsi que d'autres catégories de personnes vulnérables, ont besoin de conseils pour pouvoir gérer leur profil et comprendre l'impact que peut avoir la publication d'une information de nature privée, afin d'éviter de se mettre en danger et de nuire à autrui.

Action

3. Les Etats membres devraient engager une collaboration avec le secteur privé et la société civile visant au respect du droit des utilisateurs à la liberté d'expression, notamment en s'engageant avec les fournisseurs de réseaux sociaux à mener les actions suivantes :

– aider les utilisateurs à comprendre les paramètres par défaut de leur profil. La configuration proposée par défaut aux utilisateurs devrait limiter l'accès de tiers à des contacts qu'ils ont eux-mêmes sélectionnés[1]. Les utilisateurs devraient pouvoir prendre une décision éclairée pour autoriser l'accès à leurs données à un public plus vaste, notamment en ce qui concerne l'indexage de leur profil par des moteurs de recherche externes. A cet égard, le service de réseau social devrait :

– informer les utilisateurs des effets d'un accès illimité à leurs profil et communications (dans le temps et géographiquement), en particulier en expliquant clairement la différence entre communication privée et communication publique, ainsi que les conséquences de rendre une information publiquement disponible, y compris l'accès sans restriction à leurs données par des tiers, ainsi que la collecte de ces données ;

– informer clairement les utilisateurs, en leur offrant des outils accessibles, qu'ils ont le droit de limiter l'accès à leurs données, ainsi que le droit de les supprimer des archives et des fichiers temporaires des moteurs de recherche ;

– offrir des possibilités adéquates et bien conçues permettant à l'utilisateur de pouvoir consentir (*opt in*) à un accès plus large de tiers ;

– permettre aux utilisateurs d'exercer un contrôle sur leurs informations. Cela implique que les utilisateurs doivent être informés de la nécessité d'obtenir le consentement préalable d'autres personnes avant de publier des données à caractère personnel sur elles, y compris des contenus audio et vidéo, dans les cas où ils ont élargi l'accès des informations au-delà du cercle restreint des contacts qu'ils ont eux-mêmes sélectionnés ; sur la manière de supprimer totalement leur profil et l'ensemble des données stockées qui les concernent ou qu'ils ont envoyées sur un service de réseau social et, enfin, sur l'utilisation de pseudonymes. Les utilisateurs devraient toujours avoir la possibilité de retirer le consentement qu'ils ont donné au traitement de leurs données à caractère personnel. Avant de clôturer leur compte, les utilisateurs devraient être en mesure de transférer, aisément et librement et dans un format exploitable, les données qu'ils ont téléchargées vers un autre service ou un outil périphérique. Une fois la résiliation validée, toutes les données relatives à l'utilisateur du compte concerné devraient être définitivement supprimées du support de stockage du service de réseau social. Lorsque des applications tierces sont autorisées à accéder aux données à caractère personnel des utilisateurs, les services devraient proposer suffisamment de types d'accès de plusieurs niveaux (« *multi-layered* ») de manière à ce que les utilisateurs puissent spécifiquement consentir à l'accès à différentes catégories de données ;

– aider les utilisateurs à faire des choix éclairés sur leur identité en ligne. L'utilisation de profils avec pseudonyme représente à la fois des bénéfices 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 qu'« 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 ». Le droit d'utiliser un pseudonyme devrait être garanti à la fois au regard de la liberté d'expression et du droit de communiquer et de recevoir des informations et des idées, et du droit au respect de la vie privée. Lorsqu'un service de réseau social exige une identité réelle pour s'enregistrer sur son site, la diffusion de l'identité des utilisateurs sur internet devrait être facultative. Cela n'empêche pas pour autant les autorités chargées de l'application de la loi d'avoir accès à la véritable identité d'un internaute lorsque cela s'avère nécessaire et sous réserve de conformité aux garanties juridiques appropriées garantissant le respect des droits et des libertés fondamentales ;

– fournir aux utilisateurs des explications concises sur les conditions générales des services de réseaux sociaux, dans un langage et une forme adaptés et aisément compréhensibles par les groupes ciblés par les services de réseaux sociaux ;

– informer clairement les utilisateurs sur la politique éditoriale du fournisseur de service de réseau social en ce qui concerne ses modalités de traitement de contenus apparemment illicites et ce qu'il considère comme un contenu ou un comportement inapproprié sur le réseau.

4. De plus, les Etats membres devraient :

– encourager les initiatives de sensibilisation destinées aux parents, aux éducateurs et aux personnes chargées de mineurs en vue de compléter les informations fournies par le service de réseau social, notamment à l'égard des enfants les plus jeunes qui pourraient utiliser ce service.

[1] Voir l'Avis 5/2009 du Groupe de travail Article 29 sur les réseaux sociaux, du 12 juin 2009 ; 30e Conférence internationale des Commissaires à la protection des données et de la vie privée, Résolution sur la protection de la vie privée dans les services de réseaux sociaux (Strasbourg, 17 octobre 2008) ; « Mémorandum de Rome » du Groupe de travail international sur la protection des données dans les télécommunications (GTIPDT), Rome (3-4 mars 2008).

II. Protection des enfants et des jeunes contre les contenus ou comportements préjudiciables

Contexte et défis

5. La liberté d'expression comprend la liberté de diffuser et de recevoir des informations qui peuvent être choquantes, troublantes et insultantes. Les contenus inadaptés à certains groupes d'âge peuvent également bénéficier de la protection de l'article 10 de la Convention européenne des droits de l'homme, bien que leur diffusion soit soumise à conditions.

6. Les réseaux de services sociaux jouent un rôle de plus en plus important dans la vie des enfants et des jeunes, en contribuant au développement de leur personnalité et de leur identité, ainsi qu'à leur participation à des débats et à des activités sociales.

7. Dans ce contexte, les enfants et les jeunes devraient être protégés en raison de la vulnérabilité inhérente à leur âge. Les parents, les éducateurs et les personnes chargées de mineurs devraient jouer un rôle prépondérant dans leur rapport avec les enfants et les jeunes pour s'assurer que ces derniers utilisent ces services d'une manière appropriée.

8. Bien qu'ils ne soient pas tenus de contrôler, de surveiller et/ou de classer l'ensemble des contenus téléchargés par les utilisateurs, les fournisseurs de services de réseaux sociaux peuvent être tenus d'adopter certaines mesures préventives (par exemple, comparables aux dispositions applicables aux contenus « réservés aux adultes » dans certains Etats membres) ou de réagir avec diligence à toute réclamation (modération *a posteriori*).

9. Les mécanismes de vérification de l'âge sont habituellement présentés comme un moyen possible de protéger les enfants et les jeunes de contenus susceptibles de leur être préjudiciables. Toutefois, il n'existe pas actuellement de solution technique unique en ligne pour vérifier l'âge, qui ne porte pas atteinte à d'autres droits de l'homme et/ou n'est pas exposée à la falsification de l'âge.

Action

10. En collaboration avec le secteur privé et la société civile, les Etats membres devraient prendre des mesures appropriées pour assurer la sécurité des enfants et des jeunes, et la protection de leur dignité, tout en respectant également les garanties de procédure et le droit à la liberté d'expression et à l'accès à l'information, notamment en s'engageant avec les fournisseurs de réseaux sociaux à mener les actions suivantes :

– préciser clairement les types de contenus ou de partage de contenus ou de comportements susceptibles de porter atteinte aux dispositions légales applicables ;

– développer des politiques éditoriales de telle sorte que des contenus ou des comportements puissent être définis comme « inappropriés » selon les conditions générales d'utilisation du service de réseau social, tout en veillant à ce que cette approche ne limite pas le droit à la liberté d'expression et d'information tel que consacré par la Convention européenne des droits de l'homme ;

– créer des mécanismes aisément accessibles visant à signaler tout contenu ou comportement inapproprié ou apparemment illicite sur des réseaux sociaux ;

– partager les meilleures pratiques destinées à la prévention du harcèlement et de la sollicitation en ligne. A ce titre, il conviendrait de traiter prudemment l'accès en fonction de l'âge, dans la mesure où cette information est fournie par les enfants et les jeunes eux-mêmes. Les fournisseurs de réseaux sociaux devraient réagir avec diligence à toute plainte concernant le harcèlement ou la sollicitation en ligne.

11. De plus, les Etats membres devraient :

– encourager la mise en place de mécanismes de coopération transparents destinés aux autorités chargées de l'application de la loi et aux services de réseaux sociaux. Ces mécanismes devraient prévoir un respect des garanties procédurales prévues aux articles 8, 10 et 11 de la Convention européenne des droits de l'homme ;

– veiller au respect de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme. Cela suppose de s'abstenir de toute mesure générale de blocage et de filtrage d'un contenu injurieux ou préjudiciable, d'une manière qui entraverait l'accès des utilisateurs au contenu en question. A cet égard, la Recommandation CM/Rec(2008)6 du Comité des Ministres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet devrait être mise en œuvre afin de

veiller à ce que toute décision de blocage ou de suppression de contenu soit prise conformément à ces principes. Il convient également d'encourager des mécanismes transparents et volontaires de filtrage individuel.

III. Données à caractère personnel et confiance dans les réseaux sociaux

Contexte et défis

12. Les services de réseaux sociaux traitent un nombre considérable de données à caractère personnel, y compris les données relatives au profil des internautes et à leur utilisation d'internet. Des tiers, comme les employeurs, les compagnies d'assurance, les autorités chargées de l'application de la loi et les services de sécurité, sont notamment susceptibles d'accéder aux données à caractère personnel publiées dans un profil.

13. Les données à caractère personnel ne devraient pas être traitées par les services de réseaux sociaux au-delà de la finalité légitime particulière pour laquelle elles ont été collectées. Ces services devraient limiter le traitement aux seules données strictement nécessaires pour parvenir à la finalité convenue et pour une durée aussi courte que possible.

14. Les services de réseaux sociaux devraient demander le consentement éclairé des utilisateurs lorsqu'ils souhaitent traiter de nouvelles données à leur sujet, partager leurs données avec d'autres catégories de personnes ou d'entreprises et/ou utiliser leurs données à des finalités autres que celles spécifiées lors de leur collecte initiale. Comme le précise la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, les utilisateurs devraient être informés de l'utilisation de leurs données personnelles à des fins de profilage. La décision de l'utilisateur (refus ou consentement) ne devrait avoir aucune incidence sur son accès au service en question. Lorsque des applications tierces permettent l'accès de tiers aux données à caractère personnel des utilisateurs, les services concernés devraient proposer suffisamment de types d'accès de plusieurs niveaux (« *multi-layered* ») de manière à ce que les utilisateurs puissent spécifiquement consentir à l'accès à différentes catégories de données.

Action

15. Outre les mesures énoncées dans la première partie de cette annexe, les Etats membres, en coopération avec le secteur privé et la société civile, devraient prendre des mesures appropriées afin de garantir le droit au respect de la vie privée des utilisateurs, notamment en s'engageant avec les fournisseurs de réseaux sociaux à mener les actions suivantes :

– promouvoir les meilleures pratiques destinées aux utilisateurs. Cela comprend une configuration par défaut qui respecte la vie privée en limitant l'accès à des contacts sélectionnés par les utilisateurs eux-mêmes, l'application des mesures de sécurité les plus adaptées, le consentement éclairé des utilisateurs préalable à la diffusion de données à caractère personnel, le partage des données à caractère personnel avec d'autres catégories de personnes ou de sociétés et/ou l'utilisation de leurs données par tout autre nouveau moyen ;

– veiller à ce que les utilisateurs puissent exercer efficacement leurs droits en leur proposant, entre autres, une interface claire et dotée suffisamment de types d'accès de plusieurs niveaux (« *multi-layered* ») de manière à ce que les utilisateurs puissent spécifiquement consentir à l'accès par des tiers à différentes catégories de données ;

– s'assurer que les données sensibles bénéficient d'une protection accrue. L'utilisation de techniques susceptibles d'avoir des répercussions significatives sur la vie privée des utilisateurs – par exemple lorsque le traitement porte sur des données sensibles ou biométriques (comme la reconnaissance faciale) – exige un niveau de protection élevé et ne devrait pas être activée par défaut ;

– veiller à ce que les mesures de sécurité les plus adaptées soient appliquées à la protection des données à caractère personnel contre tout accès illicite par des tiers. Cela devrait comprendre des mesures de cryptage de bout en bout *(end-to-end)* des communications entre l'utilisateur et le site des services de réseaux sociaux. En l'absence de disposition applicable aux infractions relatives à la sécurité des données personnelles prévoyant l'obligation de notifier les violations de sécurité, les services de réseaux sociaux devraient néanmoins signaler aux utilisateurs concernés de telles violations afin qu'ils puissent prendre des mesures préventives comme changer leur mot de passe et/ou surveiller de près leurs opérations financières (lorsque les fournisseurs disposent de leurs informations bancaires ou de carte de crédit) ;

– mettre en œuvre « le respect de la vie privée dès la conception » (« *privacy by design* »). Les services de réseaux sociaux devraient être encouragés à répondre à la nécessité de protéger les données à caractère personnel dès la phase de conception de leurs produits ou services et à évaluer en permanence les

incidences sur la vie privée de toute modification apportée à des services existants afin de renforcer la sécurité et le contrôle des données à caractère personnel des utilisateurs ;

– protéger les tiers associés à des utilisateurs de réseaux sociaux. Les personnes qui n'utilisent pas les réseaux sociaux peuvent également être affectées par des publications faites par des utilisateurs de réseaux sociaux ou par l'utilisation de leurs données à caractère personnel par le service de réseau social lui-même. Elles devraient pouvoir disposer de moyens efficaces pour exercer leurs droits sans pour autant devoir devenir membre du service en question et/ou fournir une quantité excessive de données à caractère personnel. Les fournisseurs de services de réseaux sociaux devraient s'abstenir de collecter et de traiter les données à caractère personnel de personnes qui n'utilisent pas les services qu'ils offrent, par exemple leurs adresses électroniques et leurs données biométriques (notamment les photographies). Il importe que les utilisateurs soient conscients de leurs obligations à l'égard d'autres personnes et, tout particulièrement, du fait que la publication de données à caractère personnel de tiers devrait respecter les droits de ces derniers ;

– veiller à ce que le traitement, par les autorités chargées de l'application de la loi, de données à caractère personnel provenant de réseaux sociaux respecte l'article 8 de la Convention européenne des droits de l'homme. Le respect des dispositions applicables à la protection des données à caractère personnel est essentiel. Cela inclut de veiller à ce que le traitement par les autorités chargées de l'application de la loi de données à caractère personnel provenant de l'utilisation de services de réseaux sociaux s'effectue uniquement dans un cadre juridique approprié ou à la suite d'instructions ou d'ordres spécifiques de l'autorité publique compétente, décidés conformément à la loi ;

– donner des informations claires sur la loi applicable et la juridiction concernée. Il conviendrait que les utilisateurs soient informés de la loi qui s'applique aux services des réseaux sociaux et au traitement de leurs données à caractère personnel. Les dispositions contenues dans les conditions générales d'utilisation qui permettent un choix par opportunisme ou commodité du système ou de la juridiction applicable devraient être considérées comme nulles s'il n'existe aucun lien raisonnable avec ce système ou cette juridiction ; le système ou la juridiction de l'utilisateur serait préférable lorsqu'un nombre significatif d'utilisateurs est présent sur un territoire précis ;

– sensibiliser les utilisateurs aux atteintes possibles à leurs droits fondamentaux et leur permettre de chercher réparation lorsque leurs droits ont été enfreints. Les utilisateurs devraient être informés des éventuels risques pour leur droit au respect de la vie privée, non seulement dans les conditions de base des services de réseaux sociaux (y compris lorsque des modifications sont apportées aux conditions générales du service), mais aussi à chaque fois qu'un tel risque se présente, par exemple, lorsque les utilisateurs mettent à disposition de nouveaux utilisateurs (ou groupes d'utilisateurs) des informations relatives à leur profil ou lorsqu'ils installent une application tierce.

Les utilisateurs devraient être informés, de manière claire et compréhensible, et dans un langage adapté au destinataire, du traitement de leurs données à caractère personnel, ainsi que de l'existence de droits (d'accès, de rectification et d'effacement) et des moyens de les exercer.

Outre l'application des dispositions légales, des mécanismes appropriés de traitement des réclamations devraient offrir des garanties contre les comportements abusifs d'utilisateurs, notamment en ce qui concerne l'usurpation d'identité.