GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

01189/09/FR

WP 163

Avis 5/2009 sur les réseaux sociaux en ligne

adopté le 12 juin 2009

Table des matières

Synthèse

Le présent avis se concentre sur la façon dont le fonctionnement des sites de réseautage social peut répondre aux exigences de la législation de l'UE en matière de protection des données. Il a principalement pour objectif de donner des indications aux fournisseurs de SRS quant aux mesures à mettre en place afin de garantir le respect du droit communautaire.

Cet avis souligne que les fournisseurs de SRS et, dans de nombreux cas, les fournisseurs tiers, sont responsables du traitement des données, avec les responsabilités que cela implique envers les utilisateurs de SRS. L'avis observe que bon nombre d'utilisateurs évoluent dans une sphère purement personnelle et qu'ils contactent des personnes pour gérer leurs affaires personnelles, familiales ou domestiques. L'avis estime que «l'exemption domestique» s'applique dans ces cas, qui ne sont donc pas régis par les réglementations relatives aux responsables de traitement des données. L'avis précise également dans quelles circonstances les activités d'un utilisateur de SRS ne sont pas couvertes par «l'exemption domestique». La diffusion et l'utilisation d'informations disponibles sur les SRS à des fins secondaires, non recherchées, sont une préoccupation majeure du groupe de travail «article 29». L'avis recommande une sécurité robuste et des paramètres par défaut permettant de respecter la vie privée comme point de départ idéal pour tous les services offerts. La principale source de préoccupation semble être l'accès aux informations relatives au profil. L'avis aborde également des thèmes tels que le traitement de données ou d'images sensibles, la publicité ou le marketing direct sur les SRS ainsi que les problèmes de conservation des données.

Les recommandations essentielles portent sur les obligations des fournisseurs de SRS de se conformer à la directive relative à la protection des données et sur le maintien et le renforcement des droits des utilisateurs. L'engagement primordial des fournisseurs de SRS devrait être de donner aux utilisateurs dès leur inscription des informations sur leur identité et avancer toutes les raisons pour lesquelles les données à caractère personnel sont traitées. Une attention particulière devrait également être accordée au traitement des données à caractère personnel des mineurs. Selon l'avis, les utilisateurs ne devraient pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci. De plus, l'avis considère que les SRS sont également tenus de conseiller leurs utilisateurs en ce qui concerne les droits au respect de la vie privée d'autrui.

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

vu les articles 29 et 30, paragraphes 1, point a) et 3, de ladite directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu l'article 255 du traité CE ainsi que le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

L'évolution des communautés virtuelles et des services hébergés tels que les services de réseautage social («SRS») est un phénomène relativement récent et le nombre d'utilisateurs de ces sites progresse de manière exponentielle.

Les informations personnelles publiées en ligne par un utilisateur, auxquelles s'ajoutent les données décrivant les actions et interactions de celui-ci avec d'autres personnes, peuvent donner un profil précis de ses centres d'intérêts et de ses activités. Les données à caractère personnel publiées sur les sites de réseautage social peuvent être utilisées par des tiers à des fins diverses, notamment commerciales, et peuvent présenter de grands risques tels que l'usurpation d'identité, les pertes financières, la perte d'activité économique ou de possibilités d'emploi ou l'atteinte à l'intégrité physique.

En mars 2008, le groupe de travail international sur la protection des données dans les télécommunications (Berlin) a adopté le *Memorandum de Rome*[2]. Ce mémorandum analyse les risques d'atteinte à la vie privée et à la sécurité posés par les réseaux sociaux et fournit des lignes directrices aux régulateurs, fournisseurs et utilisateurs. La résolution récemment adoptée sur la protection de la vie privée dans les services de réseaux sociaux[3] se penche aussi sur les problèmes posés par les SRS. Le groupe de travail tient également compte du document d'orientation publié en octobre 2007 par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) intitulé «*Problèmes de sécurité et recommandations pour les réseaux sociaux en ligne*»[4] destiné aux régulateurs et aux fournisseurs de réseaux sociaux.

2. Définition d'un «service de réseautage social (SRS)» et modèle commercial

Les SRS peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs. Au sens

---

1 JO L 281 du 23 novembre 1995, p. 31; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Adoptée lors de la 30ème Conférence internationale des commissaires à la protection des données et à la vie privée, à Strasbourg, le 17 octobre 2008, disponible à l'adresse suivante: http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_fr.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

juridique, les réseaux sociaux sont des services de la société de l'information, tels que définis à l'article 1er, paragraphe 2, de la directive 98/34/CE, modifiée par la directive 98/48/CE. Les SRS partagent certaines caractéristiques:

- les utilisateurs sont invités à fournir des données à caractère personnel permettant de donner une description ou un «profil».

- les SRS mettent également à disposition des outils permettant aux utilisateurs de mettre leur propre contenu en ligne (contenu généré par l'utilisateur tel que des photos, des chroniques ou des commentaires, de la musique, des vidéos ou des liens vers d'autres sites[5]);

- les «réseaux sociaux» fonctionnent grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction.

Les SRS génèrent la plupart de leurs revenus avec la publicité diffusée sur les pages web que les utilisateurs créent et auxquelles ils accèdent. Les utilisateurs qui publient sur leurs profils beaucoup d'informations concernant leurs centres d'intérêts offrent un marché précis aux publicitaires souhaitant diffuser des publicités ciblées sur la base de ces informations.

Il est donc important que les SRS opèrent en respectant les droits et les libertés des utilisateurs, qui s'attendent légitimement à ce que les données à caractère personnel qu'ils divulguent soient traitées conformément à la législation européenne et nationale concernant la protection des données et de la vie privée.

3. Application de la directive relative à la protection des données

Les dispositions de la directive relative à la protection des données s'appliquent dans la plupart des cas aux fournisseurs de SRS, même lorsque leur siège est situé en dehors de l'EEE. Le groupe de travail «article 29» renvoie à son avis précédant sur les moteurs de recherche pour des informations complémentaires concernant l'établissement et l'utilisation du matériel aux fins de l'application de la directive relative à la protection des données ainsi que pour les règles découlant du traitement des adresses IP et de l'utilisation des «cookies» ou témoins[6].

3.1 Qui est responsable du traitement des données?

Fournisseurs de SRS

Les fournisseurs de SRS sont responsables du traitement des données conformément à la directive sur la protection des données. Ils fournissent les moyens permettant de traiter les données des utilisateurs ainsi que tous les services «basiques» liés à la gestion des utilisateurs (par exemple l'enregistrement et la suppression des comptes). Les fournisseurs de SRS déterminent également la manière dont les données des utilisateurs peuvent être utilisées à des fins publicitaires ou commerciales – y compris la publicité fournie par des tiers.

Fournisseurs d'application

Les fournisseurs d'application peuvent aussi être responsables du traitement des données s'ils développent des applications qui s'exécutent en complément de celles des SRS et si les utilisateurs décident de s'en servir.

---

5 Lorsque les SRS fournissent des services de communications électroniques, les dispositions de la directive 2002/58 «vie privée et communications électroniques» s'appliquent.

6 WP148, «Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche».

Utilisateurs

Dans la plupart des cas, les utilisateurs sont considérés comme étant les personnes auxquelles les données en cause se rapportent. La directive n'impose pas les obligations d'un responsable du traitement des données à une personne qui traite des données à caractère personnel «pour l'exercice d'activités exclusivement personnelles ou domestiques» - ce qu'on appelle l'«exemption domestique». Dans certains cas, l'exemption domestique peut ne pas couvrir les activités d'un utilisateur de SRS et on peut alors considérer que l'utilisateur a endossé certaines responsabilités d'un responsable de données. Quelques exemples sont développés ci-dessous:

3.1.1. Objet et nature

La tendance croissante des SRS est le passage du «*Web 2.0 pour les loisirs»* au *«Web 2.0 pour la productivité et les services»*[7] lorsque les activités de certains utilisateurs de SRS peuvent dépasser une activité purement personnelle ou domestique, quand, par exemple, le SRS est utilisé comme une plate-forme de collaboration pour une association ou une entreprise. L'exemption ne s'applique pas si un utilisateur de SRS agit au nom d'une entreprise ou d'une association ou qu'il utilise le SRS principalement comme une plate-forme à des fins commerciales, politiques ou sociales. L'utilisateur assume alors l'entière responsabilité d'un responsable du traitement des données qui révèle des données personnelles à un autre responsable du traitement des données (SRS) et à des tiers (autres utilisateurs de SRS ou même, potentiellement, autres responsables du traitement des données ayant accès aux données). Dans de telles circonstances, l'utilisateur a besoin du consentement des personnes concernées ou d'une autre base légitime figurant dans la directive relative à la protection des données.

Le plus souvent, l'accès aux données d'un utilisateur (données du profil, messages, chroniques…) est limité aux contacts qu'il a choisis. Parfois cependant, les utilisateurs peuvent acquérir un grand nombre de contacts tiers dont certains leur sont inconnus. Un nombre élevé de contacts peut indiquer que l'exception domestique ne s'applique pas et l'utilisateur sera alors considéré comme un responsable du traitement des données.

3.1.2. Accès aux informations du profil

Les SRS devraient garantir la mise en place de paramètres par défaut respectueux de la vie privée et gratuits afin de limiter l'accès aux contacts choisis par l'utilisateur.

Lorsque l'accès aux informations du profil va au-delà des contacts choisis, notamment quand tous les membres appartenant au SRS peuvent accéder à un profil[8] ou que les données sont indexables par les moteurs de recherche, l'accès dépasse la sphère personnelle ou domestique. De même, si un utilisateur décide, en parfaite connaissance de cause, d'élargir l'accès au-delà des «amis» choisis, il endosse les responsabilités d'un responsable du traitement des données. Dans la pratique, on applique alors le même régime légal que lorsqu'une personne utilise d'autres plates-formes technologiques pour publier des données personnelles sur Internet[9]. Dans plusieurs États membres, le manque de restrictions d'accès (et donc le caractère public des données) a pour conséquence que l'application de la directive relative à la protection des

---

7 Discours de Mme Reding, Membre de la Commission européenne responsable de la Société de l'Information et des Médias à propos de l'Initiative «Futur de l'Internet» du Conseil Européen de Lisbonne (2 février 2009): «l'Internet du futur: l'Europe doit jouer un rôle majeur».

8 Ou lorsqu'il peut être prouvé que l'acceptation des contacts ne fait pas l'objet d'une sélection, c'est-à-dire si les utilisateurs acceptent des «contacts» sans se soucier des liens existants.

9 Par exemple, avec des plates-formes de publication qui ne sont pas des SRS ou avec un logiciel auto-hébergé.

données[10] signifie que l'utilisateur endosse les responsabilités d'un responsable du traitement des données.

Il faut garder à l'esprit que, même si l'exemption domestique ne s'applique pas, l'utilisateur de SRS peut bénéficier d'autres exemptions comme, par exemple, pour les activités aux seules fins de journalisme ou d'expression artistique ou littéraire. Il convient alors de concilier la liberté d'expression et le droit à la vie privée.

3.1.3 Traitement des données tierces par les utilisateurs

L'application de l'exemption domestique est également limitée par le besoin de garantir les droits des tiers, particulièrement en ce qui concerne les données sensibles. Il convient en outre de noter que, même si l'exemption domestique s'applique, la responsabilité d'un utilisateur peut être engagée en application des dispositions générales du droit civil ou pénal national (notamment diffamation, responsabilité délictuelle pour violation du droit à la personnalité, responsabilité pénale).

3.2 Sécurité et paramètres de confidentialité par défaut

Le traitement sûr des informations constitue un élément clé de confiance dans les SRS. Les responsables du traitement doivent mettre en œuvre les mesures techniques et d'organisation appropriées «tant au moment de la conception du système de traitement qu'au moment même du traitement» pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger[11].

Un élément important des paramètres de confidentialité est l'accès aux données personnelles publiées sur un profil. Si cet accès n'est pas limité, un tiers peut accéder à des détails intimes concernant les utilisateurs, que ce soit en tant que membre du SRS ou via des moteurs de recherche. Cependant, seule une minorité des utilisateurs modifie les paramètres par défaut en s'inscrivant à ce genre de service. Les SRS devraient donc mettre en place des paramètres par défaut respectueux de la vie privée, qui permettent aux utilisateurs d'accepter librement et spécifiquement que des personnes autres que leurs contacts choisis accèdent à leur profil, afin de réduire le risque d'un traitement non autorisé. Les profils à accès limité ne devraient pas être repérables par les moteurs de recherche internes, y compris par la fonction de recherche par paramètres tels que l'âge ou le lieu. Les décisions d'extension de l'accès ne doivent pas être implicites[12], par exemple avec un «opt out» fourni par le responsable du SRS.

3.3 Informations fournies par les SRS

Les fournisseurs de SRS devraient informer les utilisateurs de leur identité et des différentes raisons pour lesquelles ils traitent les données personnelles, conformément aux dispositions de l'article 10 de la directive relative à la protection des données, notamment:

- l'utilisation des données à des fins de marketing direct;

---

[10] Par contre, la Cour de justice européenne avait jugé dans son arrêt *Satamedia*, point 44, que: «*Il suit que cette dernière dérogation doit être interprétée comme se rapportant seulement aux activités effectuées au cours de la vie privée ou familiale des personnes (voir Lindqvist, point 47). Ceci ne s'applique manifestement pas aux activités de Markkinapörssi et Satamedia, dont le but est de rendre les données recueillies accessibles à un nombre illimité de personnes*».

[11] Article 17 et considérant 46 de la directive relative à la protection des données.

[12] Le Mémorandum de Rome signale des risques tels que l'idée erronée d'une communauté (p. 2), la fourniture de plus d'informations qu'on ne le pense (p.3). Une société de sécurité informatique avertit un SRS de l'accès par défaut aux membres d'un même lieu géographique: http://www.sophos.com./pressoffice/news/articles/2007/10/facebook-network.html.

- le partage éventuel des données avec des catégories spécifiques de tiers;
- un aperçu des profils: leur création et leurs principales sources de données;
- l'utilisation des données sensibles.

Le groupe de travail recommande que:

- les fournisseurs de SRS mettent en garde de façon adéquate les utilisateurs contre les risques d'atteinte à leur vie privée et à celle des autres lorsqu'ils mettent des informations en ligne sur les SRS;
- les SRS rappellent à leurs utilisateurs que mettre en ligne des informations concernant d'autres personnes peut porter atteinte à leur droit à la vie privée et à la protection des données;
- les SRS conseillent à leurs utilisateurs de ne pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci[13].

3.4 Données sensibles

Les données révèlant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que celles concernant la santé ou la vie sexuelle sont considérées comme sensibles. Les données sensibles personnelles ne peuvent être publiées sur Internet qu'avec le consentement explicite de la personne concernée ou si elle a elle-même rendu ces données publiques[14].

Dans certains États membres de l'UE, les images de personnes concernées sont considérées comme une catégorie spéciale de données personnelles puisqu'elles peuvent être utilisées pour distinguer l'origine raciale/ethnique ou pour en déduire des croyances religieuses ou des données relatives à la santé. Le groupe de travail ne considère pas, en général, les images sur Internet comme des données sensibles[15], sauf si elles sont clairement utilisées pour révéler des données sensibles sur des personnes.

En tant que responsables du traitement des données, les SRS ne peuvent pas traiter des données sensibles concernant les membres ou les non-membres du réseau sans leur consentement explicite[16]. Si un SRS fait figurer sur les formulaires d'inscription des questions portant sur des données sensibles, le SRS doit indiquer très clairement qu'il est facultatif d'y répondre.

3.5 Traiter les données des non-membres

De nombreux SRS permettent aux utilisateurs de fournir des données sur d'autres personnes, notamment d'ajouter un nom à une image, d'évaluer quelqu'un ou d'énumérer les «gens que j'ai rencontrés/je veux rencontrer» à un événement. Ce marquage peut également identifier

---

13 Ceci pourrait être facilité par des outils de gestion de marquage sur les sites Internet de réseaux sociaux, notamment en créant des espaces, sur un profil personnel, pour indiquer la présence d'un nom d'utilisateur dans des images ou vidéos marquées attendant le consentement de l'utilisateur en question, ou mettre en place des délais d'expiration pour les marquages n'ayant pas reçu le consentement de la personne marquée.

14 Les États membres peuvent prévoir des exemptions à cette règle; voir article 8, paragraphe 2, point a), deuxième phrase, et article 8, paragraphe 4, de la directive relative à la protection des données.

15 La publication d'images sur Internet suscite cependant de plus en plus d'inquiétudes en termes de respect de la vie privée vu le développement des techniques de reconnaissance faciale.

16 Le consentement doit être libre, informé et spécifique.

des non-membres. Cependant, le traitement par le SRS de ce type de données concernant des non-membres ne peut se faire que si l'un des critères visés à l'article 7 de la directive relative à la protection des données est rempli.

De plus, la création de profils de non-membres préremplis grâce à l'agrégation de données fournies indépendamment par des utilisateurs de SRS, y compris les données relationnelles déduites des carnets d'adresses en ligne, n'a aucune base juridique[17].

Même si le SRS était en mesure de contacter le non-utilisateur et de l'informer de l'existence de données personnelles le concernant, toute sollicitation électronique violerait l'interdiction prévue à l'article 13, paragraphe 4, de la directive «vie privée et communications électroniques» d'envoyer des messages électroniques non sollicités à des fins de prospection directe.

3.6 Accès de tiers au réseau

3.6.1 Accès par l'intermédiaire des SRS

En complément du service de base du SRS, la plupart des SRS proposent aux utilisateurs des applications additionnelles fournies par des concepteurs tiers, qui traitent aussi des données personnelles.

Les SRS devraient avoir les moyens de garantir que les applications tierces sont conformes aux directives relatives à la protection des données et à la protection de la vie privée dans le secteur des communications électroniques. Cela suppose, notamment, qu'ils informent les utilisateurs clairement et spécifiquement du traitement de leurs données personnelles et qu'ils aient seulement accès aux données personnelles nécessaires. Les SRS devraient donc offrir aux concepteurs tiers un accès progressif afin de limiter le mode d'accès. De plus, les SRS devraient s'assurer que les utilisateurs peuvent facilement faire part de leurs inquiétudes au sujet des applications.

3.6.2 Accès de tiers par l'intermédiaire des utilisateurs

Les SRS permettent parfois aux utilisateurs d'accéder et de mettre à jour leurs données grâce à d'autres applications. Les utilisateurs peuvent par exemple:

- lire et poster des messages de leur portable sur le réseau;
- synchroniser les coordonnées de leurs amis sur le SRS avec leur carnet d'adresses sur un ordinateur de table;
- mettre à jour automatiquement leur statut ou le lieu sur le SRS en allant sur un autre site web.

  Les SRS publient sous forme d'une «interface de programmation» (API) la façon dont ce logiciel peut être créé. Cela permet à tout tiers de créer des logiciels pour accomplir ces tâches et les utilisateurs peuvent choisir entre plusieurs prestataires tiers[18]. Lorsqu'ils proposent un API permettant l'accès aux données personnelles, les SRS devraient:

---

[17] Le considérant 38 de la directive relative à la protection des données précise: «*considérant que le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte.*" Pour certains SRS, la publication des profils de non-membres semble devenir une façon non négligeable de commercialiser leurs «services».

[18] «API» est un terme technique large, mais il est fait référence ici à l'accès au nom d'un utilisateur, c'est-à-dire que les utilisateurs doivent fournir leurs données de connexion au logiciel pour que celui-ci agisse en leur nom.

- mettre en place un niveau de détail qui laisse l'utilisateur choisir un niveau d'accès destiné aux tiers limité au seul accomplissement d'une tâche donnée.

Lorsqu'ils accèdent à des données personnelles via les API des tiers au nom d'un utilisateur, les prestataires de services tiers devraient:

- traiter et conserver les données pendant une durée n'excédant pas celle nécessaire à la réalisation d'une tâche spécifique,

- limiter les opérations sur les données des contacts importés par l'utilisateur à l'usage personnel de l'utilisateur qui les a fournies.

3.7 Bases juridiques de la prospection directe

La prospection commerciale directe constitue une partie essentielle du modèle commercial des SRS; des modèles de marketing différents peuvent être utilisés par les SRS. Toutefois, la prospection utilisant les données personnelles des utilisateurs devrait respecter les dispositions applicables de la directive relative à la protection des données et celle sur la vie privée et les communications électroniques[19].

Le *marketing contextuel* est adapté au contenu que l'utilisateur voit ou auquel il accède[20].

Le *marketing segmenté* consiste à diffuser des publicités à des groupes d'utilisateurs ciblés[21]; l'utilisateur est placé dans un groupe en fonction des informations qu'il a communiquées directement au SRS[22].

Enfin, le *marketing comportemental* sélectionne les publicités par l'observation et l'analyse des activités de l'utilisateur au cours du temps. Ces techniques peuvent être soumises à des exigences juridiques selon les bases légales applicables et les caractéristiques des techniques utilisées. Le groupe de travail préconise de ne pas utiliser de données sensibles dans les modèles publicitaires comportementaux si toutes les exigences légales ne sont pas satisfaites.

Quels que soient le modèle ou la combinaison de modèles, les publicités peuvent être diffusées soit directement par le SRS (le fournisseur de SRS exerce ici une activité de courtage), soit par un publicitaire tiers. Dans le premier cas, il n'est pas nécessaire de divulguer les données personnelles des utilisateurs aux tiers. Dans le second cas toutefois, il est possible que le publicitaire tiers manipule les données personnelles des utilisateurs, s'il traite l'adresse IP de l'utilisateur ou un cookie placé sur son ordinateur, par exemple.

3.8 Conservation des données

Les SRS n'entrent pas dans la définition des services de communications électroniques inscrite à l'article 2, sous c), de la directive-cadre (2002/21/CE). Les fournisseurs de SRS peuvent offrir des services additionnels couverts par la définition des services de communications électroniques, comme un service de messagerie électronique accessible publiquement. Les dispositions de la directive relative à la protection des données et de la directive sur la protection de la vie privée dans le secteur des communications électroniques s'y appliqueront.

---

19 Le groupe de travail envisage de traiter prochainement les différents aspects de la publicité en ligne dans un autre document.

20 Par exemple, si la page regardée mentionne le mot «Paris», la publicité diffusée peut présenter un restaurant dans cette ville.

21 Chaque groupe étant défini par une série de critères.

22 Notamment au moment de son inscription au réseau.

Certains SRS permettent à leurs utilisateurs d'envoyer des invitations à des tiers. L'interdiction d'utiliser les courriers électroniques à des fins de prospection directe ne s'applique pas aux communications personnelles. Pour se conformer à l'exception des communications personnelles, un SRS doit respecter les critères suivants:

- ni l'expéditeur ni le destinataire ne sont incités à communiquer;
- le fournisseur ne sélectionne pas les destinataires[23];
- l'identité de l'expéditeur est mentionnée clairement;
- l'expéditeur doit connaître le contenu entier du message qui sera envoyé en son nom.

Certains SRS conservent également les données d'identification des utilisateurs suspendus du service pour s'assurer qu'ils ne pourront pas se reconnecter. Ces utilisateurs doivent alors être informés qu'un tel traitement est en cours. En outre, les seules informations dont la conservation est autorisée sont les informations d'identification et non les raisons pour lesquelles ces personnes ont été suspendues. Ces informations ne devraient pas être conservées plus d'un an.

Les données personnelles fournies par un utilisateur lors de son inscription au SRS devraient être effacées dès que l'utilisateur ou le fournisseur de SRS décide de supprimer le compte[24]. De même, les informations supprimées par l'utilisateur lors de la mise à jour de son compte ne devraient pas être conservées. Les SRS devraient avertir les utilisateurs avant de procéder à ces formalités avec les moyens dont ils disposent pour les informer de ces périodes de rétention. Dans certains cas spécifiques, à des fins légales et sécuritaires, il pourrait être justifié de conserver pour une durée déterminée des données qui ont été mises à jour ou effacées et des comptes afin d'empêcher les opérations malveillantes résultant de l'usurpation d'identité et d'autres délits.

Lorsqu'un utilisateur n'utilise plus le service pendant un certain laps de temps, le profil devrait devenir inactif, c'est-à-dire qu'il ne devrait plus être visible pour les autres utilisateurs ou pour le monde extérieur et quelque temps après, les données du compte abandonné devraient être effacées. Les SRS devraient avertir les utilisateurs par tous les moyens disponibles avant de procéder à ces formalités.

3.9 Droits des utilisateurs

Les SRS devraient respecter les droits des personnes concernées par le traitement des données, conformément aux dispositions inscrites aux articles 12 et 14 de la directive relative à la protection des données.

Les droits d'accès et de rectification des utilisateurs ne sont pas limités aux utilisateurs du service mais à toute personne physique dont les données sont traitées[25]. Les membres et les non-membres des SRS doivent avoir un moyen d'exercer leur droit d'accès, de rectification et d'effacement. La page d'accueil des sites de SRS devrait clairement faire référence à l'existence d'un «bureau des réclamations» mis en place par le fournisseur de SRS pour la

---

23 C'est-à-dire qu'il est interdit d'envoyer des invitations à l'ensemble du carnet d'adresses d'un contact.

24 L'article 6, paragraphe 1, sous e), de la directive sur la protection des données dispose que les données doivent être *«conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement»*.

25 C'est notamment le cas lorsque l'adresse électronique de cette personne a été utilisée par le service de SRS pour lui envoyer une invitation.

gestion des problèmes concernant la protection des données et de la vie privée ainsi que des plaintes des membres et non-membres.

L'article 6, paragraphe 1, point c), de la directive relative à la protection des données dispose que les données à caractère personnel doivent être *«adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement»*. Dans ce contexte, on observe que le SRS peut avoir besoin d'enregistrer certaines données d'identification de ses membres, mais qu'il n'a pas besoin de diffuser leur vrai nom sur Internet. Les SRS devraient donc pouvoir justifier le fait de contraindre leurs utilisateurs à agir sous leur véritable identité plutôt que sous un pseudonyme. D'importants arguments indiquent que les SRS doivent laisser le choix aux utilisateurs à cet égard et, dans au moins un État membre, il s'agit d'une exigence légale. Ces arguments s'imposent particulièrement lorsque le SRS concerné a des membres dans le monde entier.

L'article 17 de la directive relative à la protection des données prévoit que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel. Ces mesures peuvent comprendre le contrôle d'accès ainsi que des mécanismes d'authentification susceptibles d'être mis en œuvre même si des pseudonymes sont utilisés.

4. Enfants et mineurs

Une grande partie des services de SRS est utilisée par des enfants ou des mineurs. L'avis WP147[26] du groupe de travail s'est penché sur l'application de principes de protection des données dans l'environnement scolaire et éducatif. L'avis a souligné le besoin de tenir compte du meilleur intérêt de l'enfant au sens de la Convention internationale des droits de l'enfant. Le groupe de travail veut aussi insister sur l'importance de ce principe dans le contexte des SRS.

Les autorités chargées de la protection des données ont lancé diverses initiatives intéressantes[27] dans le monde entier, qui se concentrent principalement sur la sensibilisation en matière de SRS et des risques possibles. Pour relever ces défis, le groupe de travail encourage des recherches complémentaires pour résoudre les difficultés entourant la vérification de l'âge requis et la preuve du consentement préalable.

À la lumière de ce qui précède, le groupe de travail estime qu'une stratégie pluridimensionelle résoudrait le problème de la protection des données des enfants dans le contexte des SRS. Cette stratégie multiple s'appuierait sur:

- des initiatives de sensibilisation, qui s'avèrent fondamentales pour un engagement actif de la part des enfants (via les écoles, l'insertion dans le programme scolaire de notions de base en matière de protection des données, la création d'outils éducatifs appropriés et la collaboration d'organismes nationaux compétents);

- le traitement équitable et légal des mineurs, par exemple: ne pas demander de données sensibles dans le formulaire d'abonnement, pas de prospection directe visant des mineurs, l'accord préalable des parents avant l'inscription ainsi que des niveaux adaptés permettant de séparer les communautés d'enfants et d'adultes;

---

26 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_fr.pdf

27 Par exemple, l'initiative portugaise «Dadus» http://dadus.cnpd.pt/ ou encore le «Chat Check Badge» danois http://www.fdim.dk/

- la mise en place de technologies pour la protection de la vie privée (PET) – c'est-à-dire des paramètres par défaut respectueux de la vie privée, des fenêtres pop-up d'avertissement à des étapes adaptées ainsi que des logiciels de vérification de l'âge;

- l'autoréglementation des fournisseurs afin d'encourager l'adoption de codes de bonne pratique avec des mesures d'application efficaces comportant des sanctions disciplinaires;

- si nécessaire, des mesures législatives appropriées pour décourager les pratiques déloyales et/ou frauduleuses dans le contexte des SRS.

5. Synthèse des obligations/droits

Applicabilité des directives communautaires

1. La directive relative à la protection des données s'applique généralement au traitement des données personnelles par les SRS, même si leur siège se trouve en dehors de l'EEE.

2. Les fournisseurs de SRS sont considérés comme responsables du traitement des données conformément à la directive relative à la protection des données.

3. Les fournisseurs d'application peuvent éventuellement être considérés comme responsables du traitement des données conformément à la directive relative à la protection des données.

4. Les utilisateurs sont considérés comme des personnes concernées par rapport au traitement de leurs données par les SRS.

5. Dans la plupart des cas, le traitement des données personnelles par des utilisateurs relève de l'exemption domestique. Dans certains cas, les activités d'un utilisateur ne bénéficient pas de cette exemption.

6. Les SRS n'étant pas couverts par la définition des services de communications électroniques, la directive sur la conservation des données ne s'applique pas aux SRS.

Obligations des SRS

7. Les SRS devraient informer les utilisateurs de leur identité et leur fournir des informations claires et complètes sur les raisons pour lesquelles ils ont l'intention de traiter des données personnelles ainsi que les différentes manières de procéder.

8. Les SRS devraient mettre en place des paramètres par défaut respectueux de la vie privée.

9. Les SRS devraient informer et mettre en garde leurs utilisateurs contre les risques d'atteinte à la vie privée lorsqu'ils téléchargent des données sur les SRS.

11. Les SRS devraient recommander à leurs utilisateurs de ne pas mettre en ligne des images ou des informations concernant d'autres personnes sans le consentement de celles-ci.

12. **La page d'accueil des SRS, au moins, devrait présenter un lien vers un «bureau des réclamations» destiné aux membres et aux non-membres et couvrant les problèmes de protection des données.**

13. **L'activité commerciale doit respecter les règles établies par la directive relative à la protection des données et celle sur la protection de la vie privée dans le secteur des communications électroniques.**

14. **Les SRS doivent prévoir un délai maximal de conservation des données des utilisateurs inactifs. Les comptes abandonnés doivent être supprimés.**

15. **En ce qui concerne les mineurs, les SRS devraient prendre des mesures adéquates afin de limiter les risques.**

Droits des utilisateurs

16. **Les membres ainsi que les non-membres des SRS bénéficient le cas échéant des droits des personnes concernées, conformément aux dispositions des articles 10 à 14 de la directive relative à la protection des données.**

17. **Les membres et les non-membres devraient avoir accès à une procédure de traitement des plaintes mise en place par les SRS et facile à utiliser.**

18. **En général, les utilisateurs devraient être autorisés à prendre un pseudonyme.**

Fait à Bruxelles, le 12 juin 2009

Pour le groupe de travail
Le président
Alex TÜRK