30e Conférence mondiale des Commissaires à la protection des données et de la vie privée

Strasbourg, 15-17 octobre 2008

Résolution sur la protection de la vie privée dans les services de réseaux sociaux

Rapporteur : Commissaire à la Protection des données et à la liberté de l'information de l'état de Berlin, Allemagne

Parrains : Commission Nationale de l'Informatique et des Libertés (CNIL), France
Commissaire fédéral pour la protection des données et la liberté de l'information, Allemagne ;
Autorité de protection des données personnelles, Italie ;
Autorité de protection des données, Pays Bas ;
Commissaire à la Vie privée, Nouvelle-Zélande ;
Préposé fédéral à la protection des données et de l'information (PFPDI), Suisse

Résolution

Les services de réseaux sociaux[1] sont devenus très populaires depuis plusieurs années. Ces services offrent entre autre à leurs abonnés les moyens d'interagir en fonction de profils personnels qu'ils ont eux-mêmes créés et qui encouragent à révéler des informations personnelles à un niveau sans précédent sur soi et sur les autres. Mais, si les services de réseaux sociaux offrent une nouvelle gamme de possibilités de communication et d'échange en temps réel de toutes sortes d'information, l'utilisation de ces services peut cependant menacer la vie privée de leurs utilisateurs – et d'autres personnes : des quantités sans précédent de données personnelles deviennent publiquement (et mondialement) disponibles sur ces nouveaux réseaux, y compris des images et des vidéos numériques.

Une fois publiées sur le réseau, les utilisateurs sont confrontés au risque d'une éventuelle perte de contrôle sur l'utilisation de ces données : le fondement communautaire de ces réseaux laisse penser que la publication de données personnelles n'est rien d'autre qu'un échange d'information entre amis, alors que l'information contenue dans le profil de l'utilisateur peut en fait être disponible à toute une communauté d'abonnés (qui peut comporter des millions de personnes).

Il existe actuellement très peu de protection contre la copie de toute sorte de données personnelles des profils d'utilisateurs (par d'autres membres du réseau concerné, ou par des tiers non autorisés extérieurs au réseau) et de leur utilisation ultérieure pour constituer des profils personnels ou bien même republier les données ailleurs. Il peut être très difficile, et parfois même impossible, de retirer complètement l'information du Web une fois qu'elle est publiée : même après suppression sur le site d'origine (par exemple le site de réseau social), des copies peuvent être conservées chez des tiers ou des prestataires

[1] Un service de réseau social a pour principal objet la création et la vérification des réseaux sociaux en ligne de communautés qui partagent des activités et des intérêts communs, ou qui se sentent concernées par les intérêts et les activités d'autres personnes […]. Une grande partie de ces services sont offerts principalement sur Internet et proposent un ensemble de méthodes d'interaction entre les utilisateurs […] »
Traduction de Wikipedia : http://en.wikipedia.org/wiki/Social_network_service

de service de réseaux sociaux. Les données personnelles des profils peuvent également « déborder » du réseau quand elles sont indexées par des moteurs de recherche. En outre, certains fournisseurs de service de réseaux sociaux donnent accès aux données d'utilisateurs à des tiers par des interfaces de programmation (API), ces tiers peuvent alors contrôler ces données.

Un exemple d'utilisation ultérieure qui a attiré l'attention du grand public est la pratique de consultation par les responsables de ressources humaines des profils d'utilisateur candidats ou employés: selon certains articles de presse, un tiers des responsables des ressources humaines interrogés ont admis utiliser des données extraites des services de réseaux sociaux dans leur travail, par exemple pour vérifier et/ou compléter des dossiers de candidats.

Les information contenues dans les profils et les données de connexion sont également utilisées par des fournisseurs de services de réseaux sociaux pour envoyer des messages de marketing ciblés à leurs utilisateurs.

Il est très probable que d'autres utilisations inattendues de l'information contenue dans les profils d'utilisateur émergent à l'avenir.

Parmi les autres dangers déjà identifiés figurent les risques d'usurpation d'identité, favorisés par la large disponibilité des données personnelles dans les profils et le possible piratage de profils par des tiers non autorisés. La 30e Conférence mondiale des Commissaires à la protection des données et de la vie privée rappelle que ces risques ont déjà été analysés dans le document « Rapport et Conseils sur la Vie privée dans les services de réseaux sociaux » (« Mémorandum de Rome »)[2] de la 43ème réunion du Groupe de travail international sur la protection des données dans les télécommunications (3-4 mars 2008), et dans l'avis de l'ENISA no 1 intitulé « Problèmes de Sécurité et Recommandations pour les Réseaux sociaux en ligne »[3] (octobre 2007).

Les Commissaires à la Protection des données et de la vie privée rassemblés à la Conférence Internationale sont convaincus qu'il est nécessaire, en premier lieu, de réaliser une campagne d'information poussée impliquant tous les acteurs publics et privés – des instances gouvernementales aux établissements éducatifs tels que les écoles, et des fournisseurs de services de réseaux sociaux aux associations de consommateurs et d'utilisateurs, incluant également la participation des Commissaires à la protection des données et de la vie privée eux-mêmes – pour prévenir les divers risques liés à l'utilisation des services de réseaux sociaux.

Recommandations

Étant donné la nature particulière des services et les risques à court et à long terme pour la vie privée des personnes, la Conférence formule les recommandations suivantes aux utilisateurs et aux fournisseurs de services de réseaux sociaux :

Aux utilisateurs des services de réseaux sociaux

Les organismes intéressés au bien-être des utilisateurs des réseaux sociaux (y compris les prestataires de service, les gouvernements et les instances de protection des données) devraient contribuer à informer les utilisateurs sur la façon de protéger leurs données personnelles et communiquer les messages suivants.

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491
[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf (en anglais)

1. Publication d'information
Les utilisateurs des services de réseaux sociaux devraient réfléchir soigneusement aux données personnelles qu'ils publient dans leur profil. Ils devraient garder à l'esprit qu'ils peuvent être confrontés ultérieurement à ces informations ou ces images, par exemple dans une situation de recherche d'emploi. En particulier, les mineurs devraient éviter d'indiquer leur adresse personnelle ou leur numéro de téléphone.

Les personnes devraient réfléchir à l'intérêt d'utiliser un pseudonyme au lieu de leur nom réel dans un profil. Ils devraient néanmoins garder à l'esprit que l'utilisation de pseudonymes n'offre qu'une protection limitée, car des tiers peuvent être en mesure de déterminer qui est l'utilisateur d'un pseudonyme.

2. Vie privée des autres
Les utilisateurs devraient également respecter la vie privée des autres. Ils doivent être vigilants lorsqu'ils publient les informations personnelles d'une autre personne (y compris des photos, voire des photos "taggées") sans son consentement.

Aux fournisseurs de services de réseaux sociaux

Les fournisseurs de services de réseaux sociaux ont une responsabilité spéciale, ils doivent prendre en considération l'intérêt des personnes qui utilisent ces réseaux sociaux, et agir en ce sens. Outre le respect de la législation sur la protection des données, ils devraient également mettre en œuvre les recommandations suivantes.

1. Règlements et normes concernant la vie privée

Les fournisseurs en activité dans différents pays, voire au niveau mondial, devraient respecter les normes de la vie privée des pays où fonctionnent leurs services. À cet effet, ils devraient consulter les instances de protection des données selon les besoins.

2. Données personnelles de l'utilisateur
Les fournisseurs de services de réseaux sociaux devraient informer leurs utilisateurs sur le traitement de leurs données personnelles, de façon transparente et ouverte. Ils doivent également fournir une information loyale et claire sur les conséquences possibles de la publication de données personnelles dans un profil et sur les autres risques de sécurité, ainsi que sur l'éventuel accès par des tiers prévus par la loi (dont la police). L'information doit également comporter des conseils sur la façon dont les utilisateurs devraient traiter les données personnelles de tiers qu'ils diffusent sur leur propre profil.

3. Contrôle exercé par l'utilisateur
Les fournisseurs devraient également améliorer le contrôle par les utilisateurs sur l'utilisation de leurs données de profil par des membres de la même communauté. Ils devraient permettre aux utilisateurs de restreindre la diffusion de l'ensemble de leur profil ou de données y figurant, ainsi que le référencement par le moteur de recherche du réseau social.

Les fournisseurs devraient également permettre aux utilisateurs de contrôler l'utilisation ultérieure des données contenues dans leur profil et des données de connexion *;* par exemple pour le marketing ciblé. Ils devraient au minimum garantir l'opt-out pour les données non sensibles du profil, et l'opt-in pour les données sensibles (par exemple les opinions politiques ou l'orientation sexuelle) et les données de connexion.

4. Paramétrage par défaut favorable à la vie privée
En outre, les fournisseurs devraient assurer un paramétrage par défaut garantissant la protection des informations du profil de l'utilisateur. Le paramétrage par défaut a un rôle important dans la protection de la vie privée des utilisateurs : On sait que seule une minorité des utilisateurs s'inscrivant à un réseau social modifiera ultérieurement les données enregistrées lors de l'inscription. Ce paramétrage devrait être d'autant plus restrictif lorsque le service s'adresse aux mineurs.

5. Sécurité
Les fournisseurs devraient continuer à améliorer et maintenir la sécurité de leurs systèmes d'information et à protéger les utilisateurs contre l'accès frauduleux à leur profil, en appliquant les bonnes pratiques de planification, développement et exécution de leurs applications, incluant des audits et de la labellisation.

6. Droits d'accès
Les fournisseurs devraient donner aux personnes (qu'elles soient membres du réseau social ou non) le droit d'accéder à toutes leurs données personnelles détenues par le fournisseur et, le cas échéant, de les corriger.

7. Suppression des profils d'utilisateur
Les fournisseurs devraient permettre aux utilisateurs de résilier facilement leur adhésion, d'effacer leur profil et tout contenu ou toute information qu'ils ont publié sur le réseau social.

8. Utilisation du service sous pseudonyme
Les fournisseurs devraient permettre la création et l'utilisation optionnelles de profils pseudonymisés, et en encourager l'utilisation.

9. Accès par des tiers
Les fournisseurs devraient prendre des mesures efficaces pour empêcher l'aspiration (*spidering*) et/ou les téléchargements de masse (*bulk harvesting*) des données de profil par des tiers

10. Indexabilité des profils d'utilisateur
Les fournisseurs devraient veiller à ce que les données d'un utilisateur ne puissent être parcourues par des moteurs de recherche externes que si l'utilisateur a donné son consentement explicite, préalable et informé. Par défaut, les profils ne devraient pas être indexables par des moteurs de recherche.