

Vrije Universiteit Brussel

From the Selected Works of Serge Gutwirth

2008

Privacy 2.0 ?

Gloria González Fuster
Serge Gutwirth



Available at: https://works.bepress.com/serge_gutwirth/12/

Published article

GONZALES FUSTER G. & GUTWIRTH S, 'Privacy 2.0 ?', *Revue du droit des Technologies de l'Information, Doctrine*, **2008**, 349-359

Please, do always refer to the published version

Privacy 2.0 ?

Gloria González Fuster¹
Serge Gutwirth²

1. Introduction.....	2
2. Vie privée + « Web 2.0 » = « zero privacy » ?	2
2.1. Prolifération des données fournies activement par les utilisateurs	2
2.2. Prolifération des données fournies passivement par les utilisateurs	3
2.3. Informations sur la « vie privée » partielles, trompeuses ou erronées	5
2.4. Normes applicables floues	6
2.5. Limitation du droit d'accès	7
2.6. Agrégation de dossiers	7
2.7 Applications émanant de tiers.....	7
2.8 Etiquettes et « métadonnées »	8
2.9 Recherche par le contenu	8
2.10 Data mining et profiling pour des pratiques de marketing renforcées	9
3. Nouvelles pratiques, encore plus de risques ?	9
3.1 Les « communautés virtuelles mobiles »	10
3.2 Convergence, « web 2.0 » et confidentialité des communications.....	10
3.3 « L'Internet des objets » et les identifiants d'objets	10
4. Conclusion : faut-il développer des nouvelles approches ?.....	11
5. Références	12

¹ Chercheuse, *Law Science Technology and Society* (LSTS) et *Institute for European Studies* (IES), Vrije Universiteit Brussel (www.vub.ac.be/LSTS ; <http://www.ies.be/>).

² Professeur de droit, *Law Science Technology and Society* (LSTS), Faculté de droit et de criminologie, Vrije Universiteit Brussel (www.vub.ac.be/LSTS).

1. Introduction

Les différentes pratiques qui sont généralement regroupées sous le terme « web 2.0 » représentent sans aucun doute un défi majeur pour la protection de la vie privée et la protection de données personnelles. Ce défi ne découle cependant pas que des traits particuliers du phénomène « web 2.0 » en tant que tel, c'est-à-dire, en tant que phénomène reposant sur la participation active des utilisateurs à la création et au fonctionnement de sites ou applications. Il est aussi fortement lié au fait que le « web 2.0 » se place au cœur d'une dynamique globale de numérisation croissante aussi bien des communications que de la production de « contenu », dans le contexte notamment de la convergence des médias.

Cet article a pour ambition de proposer un panorama des principales implications du « web 2.0 » pour la vie privée et la protection des données en tant qu'élément de cette dynamique globale. Ainsi, il identifie en premier lieu une série de risques liés aux sites et applications tels qu'ils existent actuellement (section 2) ; en deuxième lieu, il présente quelques tendances qui peuvent prendre de l'ampleur dans le cadre de pratiques liées aux « web 2.0 » dans un futur proche (section 3).

Finalement, sont proposées des pistes à développer pour une meilleure protection de la vie privée et des données personnelles dans le contexte du « web 2.0 » et de son développement futur.

2. Vie privée + « Web 2.0 » = « *zero privacy* » ?

Quelles sont les principales « menaces » pour la vie privée et la protection de données personnelles des applications « web 2.0 » telles que nous les connaissons actuellement ? Cette section identifie les risques majeurs dans ce contexte.

Il convient de signaler que l'analyse utilise comme référence des applications « web 2.0 » au sens large : même si on peut essayer de différencier les sites orientés principalement vers les réseaux sociaux (du type Facebook) des sites qui reposent essentiellement sur l'offre de « contenu » généré par les utilisateurs (comme YouTube), en pratique un grand nombre ont une nature hybride (certains de manière très claire, comme MySpace ou Fotolog, par exemple).

2.1. Prolifération des données fournies activement par les utilisateurs

La prolifération des données mises en réseaux par l'utilisateur est une conséquence directe d'un des principes fondateurs du « web 2.0 » : le principe de la participation active. Le fait que l'utilisateur fournisse de façon libre des données personnelles le concernant ne constitue pas en soi un problème en termes de protection de la vie privée et des données personnelles : c'est bien entendu son plus grand droit.

Cependant, des risques peuvent surgir (et surgissent de fait) par rapport à : (a) la divulgation non spontanée de données ; (b) la divulgation de données personnelles concernant des tiers.

(a) Même si la participation aux réseaux « web 2.0 » est libre, dès que l'utilisateur décide d'y accéder (par exemple, suite à une invitation reçue de la part d'une connaissance ou d'un « ami »), il peut être invité, avec des degrés divers d'insistance, à fournir des données qu'il ne fournirait pas de façon spontanée. Les arguments utilisés afin de provoquer la divulgation peuvent être de diverse nature : pour des motifs de sécurité, pour « améliorer le service », etc. Le libre choix de l'utilisateur (et, par conséquent, la validité de son « consentement ») peut être affecté par une information partielle ou erronée. Permettre l'accès seulement après la révélation de certaines données pose en soi un problème pour la validité du « consentement ».

(b) L'utilisateur fournit parfois de façon directe ou indirecte des données concernant des tiers, à l'insu de ces derniers. Une des pratiques les plus courantes est la mise à disposition du fournisseur d'un réseau social du carnet d'adresses électronique de l'utilisateur, avec l'autorisation pour en faire usage. D'autres cas de figure incluent aussi, notamment, la divulgation d'informations par des mineurs sur les membres de leur famille.³

En tout cas, l'utilisateur de sites et applications « web 2.0 » ne fournit pas que des données introduites dans le système de façon active et volontaire : il est souvent incité, voire contraint, à en faire plus qu'il n'en voudrait.

2.2. Prolifération des données fournies passivement par les utilisateurs

En utilisant ces sites et applications, l'utilisateur acquiesce aussi, en général, et de façon plus ou moins consciente, au traitement des données concernant son comportement sur le site, ou vis-à-vis de l'application spécifique. En pratique, cela se traduit dans la plupart des cas en contrôle et enregistrement continus de tous ses gestes et activités en ligne lorsqu'il utilise le service : seront enregistrés et traités par exemple tous ses mouvements à travers le réseau, le contenu accédé (par exemple les « profils » des autres utilisateurs avec qui il a affaire, les chansons écoutées, les vidéos regardées, etc.), l'heure et durée de connexion, le type de navigateur, le lieu (tel qu'il peut être déduit de l'adresse dite Internet Protocol (IP)). Certains auteurs

³ L'affaire *Lindqvist* a déjà permis à la Cour de justice des Communautés européennes (C.J.C.E) de s'attaquer à des problèmes similaires, quoique dans un scénario « web 1.0 » (mise en ligne de données sensibles par un tiers) (C.J.C.E, arrêt du 6 novembre 2003, *Bodil Lindqvist*, C-101/1). Voir, sur cet arrêt : L. COUDRAY, «Case C-101/01, Bodil Lindqvist», *Common Market Law Review*, 2004, 41, pp. 1361-1376.

nomment cette menace la « collecte secondaire de données », et la situent parmi les principaux risques liés aux communautés virtuelles⁴.

Ces informations sont récoltées afin de créer des profils d'utilisateurs, dans la plupart des cas à des fins de *marketing*. Il convient de souligner que ces données sont normalement récoltées de façon centralisée par le fournisseur du « service » (càd par l'entité qui fera de la publicité et du marketing, dans la plupart des cas). La conception de sites et applications « web 2.0 » sous forme de « communautés » tend à accentuer l'importance des interactions entre utilisateurs. Cependant cette notion peut être considérée généralement comme trompeuse puisqu'elle néglige l'importance du fournisseur du service et sa place privilégiée dans la soi-disant « communauté ». Même dans des systèmes basés sur des logiques *peer-to-peer* (ou p2p), les traitements de données se font très souvent de façon centralisée.

Les données collectées incluent notamment des adresses IP, considérées comme des « données de trafic » dans le cadre de la législation européenne en matière de communications électroniques. En tant que telles, elles sont soumises à des règles spécifiques instaurées par la Directive 2002/58/EC⁵. Mais comme ces règles spécifiques s'appliquent exclusivement aux fournisseurs de services de communications électroniques au sens du droit communautaire, et que les entités qui les collectent et en assurent le traitement dans le cadre de services « web 2.0 » n'en sont généralement pas, le traitement d'adresses IP par des fournisseurs de services « web 2.0 » ne seront pas soumis à la protection spéciale des « données de trafic ».

D'autre part, ces adresses IP doivent-elles être protégées en tant que « données personnelles » ? C'est une question qui a suscité de nombreux débats. Les fournisseurs de services « web 2.0 » ont tendance à nier le caractère de « donnée personnelle » de l'adresse IP et, par conséquent, refusent de se considérer « responsables du traitement » de données personnelles au sens de l'article 2(b) de la Directive 95/46/CE, et d'assumer les obligations qui en découlent.

Selon l'article 2(a) de la Directive 95/46/EC⁶, reprise par l'article 2(a) de la Directive 2002/58/CE, doit être qualifiée de « donnée à caractère personnel » « *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».

Le « Groupe de protection des personnes à l'égard du traitement des données à caractère personnel » crée par l'Article 29 de la Directive 95/46/EC a émis l'opinion que les fournisseurs de services Internet (comme, par exemple, de services de moteurs de recherche⁷) doivent impérativement traiter les adresses IP comme des données

⁴ G. HOGBEN (ed.), *Security Issues and Recommendations for Online Social Networks*, ENISA Position Paper No. 1, European Network and Information Security Agency (ENISA), Heraklion, Octobre 2007, p. 3.

⁵ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *Journal officiel des Communautés européennes*, n° L 201 du 31/07/2002, pp. 37-47.

⁶ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel des Communautés européennes*, n° L 281 du 23/11/1995, pp. 31-50.

⁷ Article 29 Working Party (2008), *Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)*, WP150, May 15, p. 6.

personnelles, sauf dans les cas où ils seraient en mesure de démontrer que ces données concernent des utilisateurs qui ne peuvent pas être identifiés. En outre, le Groupe considère que des données peuvent « *concerner quelqu'un* » soit en raison de leur contenu (les données sont à propos de quelqu'un), soit en raison de leur finalité (les données sont traitées pour quelqu'un), ou encore en raison de leur impact (les données vont avoir un effet sur quelqu'un)⁸. Ce raisonnement et la définition très large qui en découle permet en théorie de couvrir un très large éventail de traitements de données. Or, en termes pratiques, l'approche du Groupe de l'Article 29 a le désavantage d'être systématiquement ignorée par les fournisseurs de services, qui optent pour des définitions bien plus *minimalistes* de la notion de « donnée personnelle ». Le traitement massif d'adresses IP par les fournisseurs de services de réseaux sociaux a en tout cas été identifié comme une des menaces majeures pour la vie privée dans ce contexte⁹.

2.3. Informations sur la « vie privée » partielles, trompeuses ou erronées

Les sites les plus populaires ne manquent pas de faire référence à leurs efforts en matière de protection de la « privacy » de leurs utilisateurs. Le contenu des « privacy policies » qu'ils affichent mériterait sans doute de nombreuses pages d'analyse. Il convient de rappeler que ces notifications doivent être claires, non pas par courtoisie envers l'utilisateur, mais par impératif légal. L'effectivité des droits dont dispose la personne concernée va en effet dépendre de son accès effectif à une information claire à propos des traitements en cours.

Plusieurs problèmes récurrents sont à retenir :

(a) un décalage entre la notion de « privacy » dont les sites font mention et les droits à la vie privée et à la protection des données personnelles tels qu'ils sont reconnus dans le cadre de l'Union européenne. Ainsi, plusieurs « privacy policies » sont des « politiques de confidentialité », alors que la confidentialité ne couvre pas les différentes dimensions des droits mentionnés ;

(b) des « privacy settings » sont en général mis en avant comme outils destinés à protéger les utilisateurs, alors qu'en réalité ils ne sont dans la plupart des cas que des « préférences » de visibilité différente concernant une partie des informations fournies par ces utilisateurs ;

(c) l'identification des entités responsables du traitement est souvent confuse. Cela est dû, en partie, au fait que, comme signalé, certains « responsables du traitement » de données personnelles ne considèrent pas les données en question comme des « données personnelles ». Ils refusent donc d'être qualifiés de « responsables du traitement » et ne se présentent pas comme tels.

⁸ Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP136, June 20, p. 10.

⁹ International Working Group (IWG) on Data Protection in Telecommunications (2008), *Report and Guidance on Privacy in Social Networks Services*, 'Rome memorandum', 43rd Meeting, Rome, 3-4 March, p. 2.

Des exemples d'interprétations créatives de ces notions ne manquent pas. Ainsi, le fournisseur du réseau social MySpace distingue les « *données d'inscription* » communiquées obligatoirement lors de l'inscription (adresse électronique, nom et prénom, code postal, sexe et date de naissance) et les « *informations de profil* » librement introduites par l'utilisateur (intérêts, hobbies, style de vie, groupes d'affiliation, vidéos et/ou photos, messages privés, bulletins ou déclarations personnelles). Ensuite, il affirme que « *MySpace détermine les finalités de la collecte, l'utilisation et la divulgation des Données d'Inscription que vous fournissez et, en tant que tel, fait office de responsable du traitement de telles données. Etant donné que seul le Membre, et non MySpace, détermine les finalités de la collecte, l'utilisation et la divulgation des Informations du Profil, MySpace n'a pas la qualité de responsable du traitement des Informations du Profil mises en ligne par les Membres* »¹⁰.

2.4. Normes applicables floues

La plupart des fournisseurs de services « web 2.0 », très populaires sur le territoire de l'UE, se présentent comme étant basés ailleurs (le plus souvent, aux Etats-Unis). En conséquence ils n'appliquent pas directement les normes européennes en matière de protection de données personnelles. Les entités basées aux Etats-Unis peuvent traiter des données personnelles collectées dans l'UE en se soumettant à une série de contraintes, reprises dans l'accord dit « Safe Harbor », notamment à travers des programmes comme TRUSTe.

A la rubrique « politique d'information », Facebook affirme agir en accord avec le programme TRUSTe et les principes de l'accord « Safe Harbor ». Ensuite, l'avertissement suivant apparaît : « *Veillez noter que vous publiez sur ce site des informations (comme défini dans les Conditions d'utilisation de Facebook) à vos risques et périls* »¹¹.

Des problèmes de contradiction entre les obligations en matière de droit à la protection de données en droit communautaire et d'autres obligations peuvent surgir. Ainsi, MySpace met en garde ses utilisateurs : « *Si vous en faites la demande à MySpace, celle-ci cessera d'utiliser vos IPI, mais conservera un dossier de vos IPI nécessaires pour être en conformité avec les lois et règlements en vigueur* ». On peut imaginer qu'il s'agisse des lois et règlements en vigueur aux Etats-Unis, pays où sont hébergés les services de MySpace.

Il a été souligné que les fournisseurs des services Internet qui opèrent sur plusieurs pays ou mondialement, et notamment ceux qui proposent des services de réseaux sociaux, devraient respecter les normes applicables dans les pays où ils offrent leurs services¹².

¹⁰ *Politique de confidentialité de MySpace* pour MySpace France (entrée en vigueur : 28.02.2008), <http://www.myspace.com/index.cfm?fuseaction=misc.privacy> (dernière consultation : 27/06/2008).

¹¹ *Politique de Confidentialité de Facebook* (en vigueur à partir du 6 décembre 2007, <http://fr.facebook.com/policy.php> (dernière consultation : 27/06/2008).

¹² Article 29 Working Party (2008), *Opinion on data protection issues related to search engines*, WP 148, April 4, p. 7.

2.5. Limitation du droit d'accès

Le droit d'accéder aux données personnelles peut être facilement compromis, non seulement à cause du transfert international des données et de problèmes et questions de droit applicable. Le droit d'accès et celui de rectification peuvent aussi être réduits ou anéantis pour des raisons présentées comme « techniques » ou de gestion des données par le système.

Ainsi, Facebook informe ses utilisateurs du fait que : “[v]ous comprenez et reconnaissez que, même après suppression, des copies du contenu utilisateur peuvent rester visibles dans les pages d'archives et les pages en cache ou bien si d'autres utilisateurs ont ayant (sic)¹³ enregistré ou copié votre contenu”.

2.6. Agrégation de dossiers

L'extrait qui précède omet naturellement de dire que ce ne sont pas seulement « d'autres utilisateurs » qui peuvent copier les informations disponibles sur un utilisateur dans le cadre d'un service « web 2.0 ». Des tiers peuvent aussi y avoir accès, avec ou sans le consentement de la personne concernée.

La pratique dite d'« agrégation de dossiers » permet par exemple d'intégrer les données traitées dans le cadre d'une application dans une autre. Elle permet aussi d'obtenir des informations supplémentaires à partir d'un ensemble d'informations qui n'étaient peut-être pas censées se rejoindre à l'origine. L'« agrégation de dossiers » a été identifiée comme une des principales menaces pour la vie privée liées aux réseaux sociaux par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)¹⁴.

2.7 Applications émanant de tiers

Les services de type « web 2.0 » ne peuvent pas être envisagés comme des services qui opèrent isolément. En partie justement à cause de leur nature « ouverte », facilitant la participation active, ils peuvent aisément accepter que des applications créées ou opérées par des tiers soient activées dans le cadre de leurs services.

Cette co-existence de services produit souvent un entremêlement de responsabilités, où le seul fait qui est clair en fin de compte est, en général, que le service de base refuse toute responsabilité par rapport aux traitements de données opérés par des applications de tiers (dont les responsables ont aussi tendance à décliner toute responsabilité). Des questions de sécurité peuvent être spécialement importantes dans ce contexte.

¹³ La version française de la politique de confidentialité de Facebook (voir note 11) est officiellement proposée sur le site « *uniquement à titre indicatif* », la version en anglais étant « *la seule à faire foi et la seule qui engage les deux Parties* ». La texte en français inclut non seulement des nombreuses fautes, mais aussi des phrases inachevées (par exemple : « *En plus, nous stockons certaines informations de votre navigateur en utilisant des.* »).

¹⁴ G. HOGBEN (ed.), *Security Issues and Recommendations for Online Social Networks*, ENISA Position Paper No. 1, European Network and Information Security Agency (ENISA), Heraklion, Octobre 2007, p. 3.

2.8 Etiquettes et « métadonnées »

Le phénomène de l' « étiquetage » a sans doute contribué en grande mesure à l'essor et au succès des services « web 2.0 ». Les « étiquettes » ou « tags » permettent aux utilisateurs de certains services de s'exprimer par rapport au contenu auquel ils accèdent, augmentant les informations disponibles sur celui-ci (et sur eux-mêmes). Plus dangereusement, cet « étiquetage électronique » peut aussi mettre en rapport des informations concernant des tiers, et même transformer des données qui n'étaient pas a priori des « données personnelles » en « données personnelles ». Ainsi, il est commun de placer des étiquettes portant des noms propres sur des photos de personnes qui n'étaient pas identifiables. Lorsqu'un nom est « attaché » à une photo, cette photo peut à son tour permettre d'établir un lien avec un « profil » d'un utilisateur dans un réseau, et ceci malgré le fait que le profil ait été créé sous pseudonyme¹⁵.

En général le mot « métadonnées » est utilisé pour indiquer des données « inscrites » dans des fichiers, des documents ou dans des éléments de langage de marquage. Il s'agit de marqueurs dont le but principal est de faciliter le traitement des données qu'ils marquent ; ils peuvent être introduits de façon manuelle, semi-automatique, ou automatique.

Les fichiers numériques (contenant du texte, des images, du contenu audio, vidéo ou multimédia) conservent ces « métadonnées » lors de tout traitement tel que, par exemple, la transmission ou la réplique.

L'importance de ces « métadonnées » pour la protection de la vie privée et des données personnelles est proportionnellement liée à l'importance de l'usage de fichiers numériques. Et ces fichiers ont justement un rôle très important à jouer dans le cadre de services « web 2.0 » qui stimulent l'usage de « contenu » généré par l'utilisateur et donc le recours massif à des photos, vidéos, chansons et autres fichiers fournis par les utilisateurs.

Les utilisateurs sont-ils conscients des « métadonnées » et autres étiquettes liés aux fichiers qu'ils utilisent et « partagent »? Faudrait-il préconiser une réglementation spéciale pour le traitement de ces données ? La question est à explorer.

2.9 Recherche par le contenu

Les étiquettes et les métadonnées peuvent être fort utiles pour la recherche d'informations. Néanmoins, on assiste actuellement au développement d'autres approches pour améliorer la recherche, et notamment de techniques qui permettent d'obtenir des informations à partir de l'analyse des caractéristiques visuelles des images.

La recherche d'images par le contenu [en anglais, Content Based Image Retrieval (CBIR)] comporte comme risque principal pour la protection de la vie privée et des données personnelles le fait de permettre l'extraction de données que l'on croyait absentes du fichier. Il peut s'agir des données qui rendent une personne

¹⁵ International Working Group (IWG) on Data Protection in Telecommunications (2008), *Report and Guidance on Privacy in Social Networks Services*, 'Rome memorandum', 43rd Meeting, Rome, 3-4 March, p. 3.

indentifiable ou identifiable, ou des données qui transforment le fichier en « donnée de localisation »¹⁶.

2.10 Data mining et profiling pour des pratiques de marketing renforcées

Au-delà de l'idéalisme et du romantisme social, le but ultime de la collecte et du traitement d'informations dans le cadre de la plupart de services « web 2.0 » reste le profit économique, obtenu en général à travers du marketing et de la publicité. Le déploiement de la publicité et des stratégies de marketing se traduisent notamment par des communications non sollicitées, ou des ajustements non sollicités.

Il serait probablement injuste d'affirmer que les principaux fournisseurs de services « web 2.0 » ne tiennent pas du tout compte du point de vue de ceux qui désirent réduire l'impact de ces pratiques sur leur participation. Ainsi, MySpace offre à ses utilisateurs la possibilité de « *désactiver la personnalisation des publicités réalisée à partir de vos Informations de Profil Non Structurées* ». Pour cela il suffit de s'identifier et décocher la réponse « *Afficher les publicités correspondant à mes centres d'intérêts exprimés dans mon profil (recommandé)* », et cocher la réponse « *Ne pas afficher les publicités pertinentes; je souhaite recevoir des publicités non personnalisées qui peuvent ne pas avoir d'intérêt pour moi* »¹⁷. La rédaction de ces phrases n'invite pas spécialement à désactiver la soi-disant « personnalisation », qui de toute façon pourra continuer à s'opérer sur la base d'autres données.

La gestion de la publicité n'est pas toujours mise en place par le fournisseur du service lui-même ce qui, à nouveau, peut créer des problèmes liés à la confusion des responsabilités. Ainsi, la « déclaration de confidentialité » de YouTube pour la France (il faut noter qu'il n'en existe pas pour la Belgique) signale que YouTube permet à d'autres sociétés de collecter les adresses IP des utilisateurs et de recourir à des « *cookies, JavaScript ou les balises Web* » pour fournir de la publicité. En outre, YouTube note plus concrètement qu'il entretient un partenariat avec DoubleClick à cette fin, et renvoie pour plus d'informations à ce propos vers le site de DoubleClick, accessible d'ailleurs seulement en anglais¹⁸.

3. Nouvelles pratiques, encore plus de risques ?

Cette section explore quelques tendances qui sont à prendre en compte dans les analyses de l'impact sur la vie privée et la protection des données personnelles dans le contexte des développements issus du « web 2.0 ».

¹⁶ International Working Group (IWG) on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Networks Services*, 'Rome memorandum', 43rd Meeting, Rome, 3-4 March 2008, p. 3.

¹⁷ Reprises ici; <http://www.myspace.com/index.cfm?fuseaction=accountsettings.profiletargeting> (dernière consultation : 27/06/2008).

¹⁸ *Déclaration de confidentialité YouTube* (mise à jour : 27 février 2008), <http://fr.youtube.com/t/privacy> (dernière consultation : 27/06/2008).

3.1 Les « communautés virtuelles mobiles »

Les soi-disant « communautés virtuelles mobiles » sont des réseaux construits à partir d'échanges réalisés avec des téléphones portables. Elles ne doivent donc pas forcément être « mobiles », ni vraiment « virtuelles » et ne sont bien entendu des « communautés » que de façon relative. Ce qui présente de l'intérêt du point de vue de la protection de la vie privée et de la protection des données, c'est est que le traitement de données inclut ici systématiquement des données dites « de trafic » et de « localisation ». Celles-ci jouissent d'un régime de protection spéciale établi au niveau communautaire par la Directive 2002/58/EC, dont le champ d'application est cependant limité, comme nous l'avons déjà signalé à propos des limites de la protection des adresses IP en tant que « données de trafic ».

Le traitement de données de localisation a connu une croissance exponentielle ces dernières années, notamment à la suite de la prolifération de l'usage de données satellite et de la téléphonie mobile¹⁹. Les services qui reposent sur le traitement de ce type de données sont soumis à des conditions spéciales, visant à garantir, entre autres, la possibilité pour la personne concernée de choisir à tout moment de cesser d'émettre ce type de données. Il semble très important de veiller au maintien de ce principe dans le contexte du développement de « communautés virtuelles mobiles », et surtout à éviter qu'il puisse être compromis par un recours abusif au consentement de l'utilisateur.

3.2 Convergence, « web 2.0 » et confidentialité des communications

Les « communautés virtuelles mobiles » peuvent fournir, entre autres, des services de communication entre les utilisateurs. Cela peut donner lieu à des services qui ressemblent à s'y méprendre à des communications téléphoniques « traditionnelles ». *Quid* de la confidentialité des communications dans ces cas ? Les fournisseurs de services « web 2.0 » prendraient-ils en charge la responsabilité de la faire respecter ? L'envoi de messages électroniques dans le contexte de réseaux sociaux pose déjà des problèmes dans la même perspective, des pratiques de *screening*, très critiquées, pouvant avoir lieu²⁰.

3.3 « L'Internet des objets » et les identifiants d'objets

La notion de « Internet des objets » fait référence à la possibilité d'augmenter le rôle des décisions automatiques prises par des différents objets dans des réseaux d'information. Pour se développer cet « Internet des objets » requiert une multiplication de la collecte de données (notamment à travers des senseurs) ; il est

¹⁹ Article 29 Working Party (2005), *Opinion on the use of location data with a view to providing value-added services*, WP 115, November, p. 2.

²⁰ Article 29 Working Party (2006), *Opinion 2/2006 on privacy issues related to the provision of email screening services*, WP 118, February 21, p. 8.

censé se développer aussi dans le cadre de la prolifération du recours à la radio identification (de l'anglais radio frequency identification (RFID)).

Un « Internet des objets » ne peut fonctionner que sur la base d'une identification au moins relativement stable des objets en question. Il a ainsi été affirmé que, dans un futur proche, tout « objet » sera doté d'un identifiant propre, probablement sous la forme d'une adresse unique. Ceci serait nécessaire pour que les échanges d'information puissent avoir lieu²¹.

Quel statut légal ces identifiants doivent-ils avoir ? Doivent-ils être assimilés à des « données de trafic » ? La protection de celle-ci doit-elle être améliorée ? Méritent-ils une protection spéciale, en particulier concernant la possible inclusion d'identifiants uniques dans de fichiers numériques en tant que « métadonnées » ?

4. Conclusion : faut-il développer des nouvelles approches ?

La protection de la vie privée et la protection des données personnelles des utilisateurs de services « web 2.0 » ne peut pas être considérée comme étant satisfaisante. Ces services et des développements connexes représentent d'ailleurs également des risques pour les non-utilisateurs.

L'ampleur du problème a stimulé de nombreux débats à ce propos²².

Le besoin de renforcer l'application du droit existant dans ce domaine semble évident. Il est clair qu'il reste beaucoup de travail sur la planche, notamment en ce qui concerne la légitimité du traitement et la qualité des informations mises à la disposition des utilisateurs ; l'effectivité des droits d'accès et de rectification ; la clarification des responsabilités ; l'instauration d'un régime de détermination du droit applicable qui favorise l'utilisateur.

Le Contrôleur européen de la protection des données a identifié comme défis principaux pour la protection en droit communautaire : a) la définition de « responsable du traitement » ; b) l'applicabilité de normes et le critère chaque fois plus relatif du lieu du traitement.

A un niveau plus fondamental il faut probablement commencer à se demander si la distinction entre les données personnelles et les autres données peut être soutenue dans le monde du « web 2.0 » et de « l'Internet des choses ». Dans un tel monde, en effet, il est devenu facile d'agir sur la conduite des individus sans avoir à les identifier. Il est donc peut-être temps de lancer l'exploration des possibilités d'une transformation de « la protection des données personnelles » en une « protection des données » *tout court, un mouvement d'ailleurs déjà perceptible dans la reconnaissance d'un régime de protection particulier pour les « données de trafic » et*

²¹ European Commission (2008), *Internet of Things in 2020: Roadmap for the Future*, INFSO D.4 Networked Enterprise & RFID, INFSO G.2 Micro & Nanosystems in cooperation with Working Group RFID of the European Technology Platform (ETP) on Smart Systems Integration (EPOSS), Version 1.1, 27 May, p. 4.

²² Différents projets de recherche dans ce domaine sont actuellement développés au niveau européen avec le soutien de la Commission européenne, comme PICOS – « Privacy and Identity Management for Community Services » (<http://www.picos-project.eu/>) ou PrimeLife, « Bringing sustainable privacy and identity management to future networks and services » (<http://www.primelife.eu>).

les « données de localisation »²³. Une telle refonte de la protection des données ne prendrait plus l'« identifiabilité » des personnes concernées comme critère, mais elle s'activerait chaque fois que des données et du savoir développés dans le cadre des nouvelles applications type « web 2.0 » et « Internet des choses » s'avèreraient avoir un impact sur nos décisions et notre conduite, en dépit de leur capacité ou non de rendre possible notre identification. En ce sens, peut être envisagée par exemple une réglementation des ajustements non sollicités, parallèle à celle déjà existante pour les communications non sollicitées.

Entre temps, une protection supplémentaire pourrait déjà être facilement mise en place à travers une régulation des données capables d'identifier les « objets » qui nous entourent : ordinateurs, téléphones portables, lecteurs mp3 et autres appareils multifonctions à venir. Ces « objets » peuvent laisser des traces inattendues sur nos communications, mais aussi sur les fruits de toutes ces activités créatives à travers lesquelles certains tentent de s'exprimer et d'interagir publiquement, notamment grâce à des sites et applications « web 2.0 » : créations littéraires, musicales, photographiques, ou audiovisuelles. Protéger les individus dans le contexte du « web 2.0 » et à l'heure de « l'Internet de choses » pourrait passer aussi par la protection de « l'anonymat des choses » ou du moins de la non-traçabilité des empreintes électroniques qu'elles laissent.

Des nouvelles stratégies s'imposent en tout cas.

5. Références

Article 29 Working Party (2005), *Opinion on the use of location data with a view to providing value-added services*, WP 115, November.

Article 29 Working Party (2006), *Opinion 2/2006 on privacy issues related to the provision of email screening services*, WP 118, February 21.

Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP136, June 20.

Article 29 Working Party (2008), *Opinion on data protection issues related to search engines*, WP 148, April 4, p. 7.

Article 29 Working Party (2008), *Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)*, WP150, May 15.

Coudray, Ludovic (2004), "Case C-101/01, Bodil Lindqvist", *Common Market Law Review*, 41, pp. 1361-1376.

Cour de justice des Communautés européennes (C.J.C.E), arrêt du 6 novembre 2003, Bodil Lindqvist, C-101/1.

²³ S. GUTWIRTH & P. DE HERT, , "Regulating profiling in a democratic constitutional state" in M. HILDEBRANDT & S. GUTWIRTH, *Profiling the European citizen. Cross disciplinary perspectives*, Springer Science, Dordrecht, 2008, p. 289.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel des Communautés européennes, n° L 281 du 23/11/1995, pp. 31-50.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), Journal officiel des Communautés européennes, n° L 201 du 31/07/2002, pp. 37-47.

Gutwirth, S. & De Hert, P. (2008), "Regulating profiling in a democratic constitutional state" in Hildebrandt, M. & Gutwirth, S., *Profiling the European citizen. Cross disciplinary perspectives*, Springer Science, Dordrecht, pp. 271-293.

Hogben, Giles (ed.) (2007), *Security Issues and Recommendations for Online Social Networks*, ENISA Position Paper No. 1, European Network and Information Security Agency (ENISA), Heraklion.

International Working Group (IWG) on Data Protection in Telecommunications (2008), *Report and Guidance on Privacy in Social Networks Services*, 'Rome memorandum', 43rd Meeting, Rome, 3-4 March.