Les réseaux sociaux menacent-ils nos libertés individuelles ?

Principes des réseaux sociaux sur Internet

Les réseaux sociaux sur Internet reprennent les principes mêmes des réseaux sociaux qui existent dans le monde physique. Toutefois, ils utilisent des ressources classiques du Web, comme la messagerie ou les forums de discussion et ils diffèrent par la rapidité de la mise en relation, la connaissance des contacts de ses contacts, la vision instantanée des actions menées sur le réseau. Ainsi ils permettent une vision en temps réel des membres de son réseau et des actions que ses contacts accomplissent (par exemple A publie tel lien sur sa page, B rentre en contact avec C).

Concrètement, outre les informations caractéristiques de son profil que l'internaute renseigne parfois avec des informations sensibles au sens de la CNIL (opinions politiques, religieuses, philosophiques, appartenance syndicale, santé, orientation sexuelle) et qui sont souvent optionnelles, le pivot d'un réseau social est pour la majorité des acteurs constitué par le carnet d'adresses du membre. Ainsi, les réseaux sociaux permettent de constituer des gigantesques bases de données sur les personnes. Facebook crée ainsi une base de données de profils qui permet des ciblages très précis connaissant le profil du consommateur, ses centres d'intérêt, etc. Le profil d'un internaute est réalisé à partir des données que celui-ci renseigne, des informations qu'il publie mais aussi de ses contacts selon l'adage « *Dis-moi qui sont tes contacts, je te dirai qui tu es* ».

Les réseaux sociaux sont au cœur du Web 2.0 qui est un web collaboratif, ayant techniquement évolué depuis la première génération du Web au début des années 1990 et qui donne la primauté aux données. Les réseaux sociaux, ne constituent pas un phénomène de mode – même si les modèles économiques de certains acteurs ne sont pas toujours mûrs, la priorité pour certains étant la course à l'audience pour fédérer une communauté d'utilisateurs et de services rendus incontournables autour, qui feront l'objet d'une monétisation lors d'une étape ultérieure. *A contrario*, ils traduisent une évolution inéluctable tant pour les organisations que pour les particuliers qui guide la croissance du Web. En effet, depuis 2 ans, les internautes toujours plus nombreux et plus longuement connectés se rendent de moins en moins sur les sites des entreprises au profil des réseaux sociaux. Et demain, les entreprises ne pourront pas ne pas être sur les réseaux sociaux comme elles ne peuvent plus se passer du téléphone ou de la messagerie aujourd'hui ! Aussi il convient de mesurer comment les libertés individuelles évoluent et se gèrent de façon à les utiliser en connaissance de cause.

Au-delà d'opportunités réelles, des risques sont à intégrer avant toute utilisation

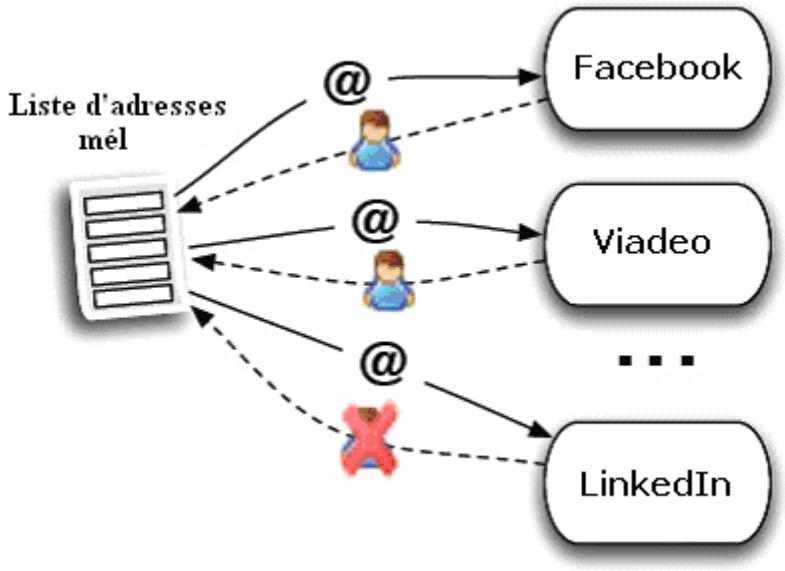
Les opportunités offertes par les réseaux sociaux sont réelles pour l'internaute (visibilité sur Internet et par exemple disposer d'un CV en ligne sur des réseaux sociaux professionnels comme LinkedIn ou Viadeo, recherche de partenaires/fournisseurs/clients, retrouvaille avec des personnes perdues de vue, recherche de personnes ayant des goûts ou intérêts communs, etc.), mais en contrepartie les risques nombreux :

1. **L'usurpation d'identité** existe. On peut endosser facilement l'identité d'un tiers. Ayant collecté sa photo sur le Web, connaissant quelques informations de nature personnelle (date de naissance, profession), la création d'un faux profil sur un réseau social donné est rapide et facile. Il est alors possible de rentrer en contact avec des personnes susceptibles de connaître la personne incarnée. Et en cas de fraude, dans bien des cas, la vraie personne doit apporter des preuves pour prouver qu'elle est bien la bonne personne. L'usurpation d'identité sur Internet est restée longtemps non condamnée du fait d'un vide juridique, semble-t-il comblé par des dispositions de la loi LOPPSI 2.

2. Les **bases de données des internautes peuvent faire l'objet de piratage** : des données stockées peuvent être indûment copiées, modifiées, effacées, vendues à des tiers. Ces risques sont accrus avec l'interopérabilité permise entre les réseaux sociaux laquelle induit de nouvelles failles même si de nouveaux processus d'identification/authentification (par exemple fonction d'import de ses contacts de messagerie vers un réseau social donné) sont mis en œuvre. Dès lors que des informations sont indûment captées, toute utilisation à des fins malveillantes est possible, le travers commercial étant de réutiliser ces données à des fins de publicités non sollicitées mais le plus gros risque étant celui d'une utilisation par un gouvernement autoritaire qui ségrégerait des catégories de citoyens en utilisant les informations dûment renseignées par les internautes eux-mêmes. En outre, des captations de mots de passe sont possibles et un tiers malveillant peut ainsi se connecter à l'insu de la véritable personne et, ayant le contrôle de son compte sur un réseau social donné, entacher sa réputation.

3. Les **données collectées** par les réseaux sociaux peuvent être **utilisées à des fins commerciales** (par exemple module Beacon de Facebook qui ayant suscité un tollé de la part des internautes a été abandonné), sachant que les conditions générales d'utilisation d'un outil peuvent changer dans le temps. Ces derniers mois, les conditions d'utilisation des sites Facebook et Twitter ont ainsi évolué à plusieurs reprises et de façon léonine, l'utilisateur ne pouvant qu'accepter les nouvelles conditions générales d'utilisation en bloc ou cesser d'utiliser le service. Le réseau social Ning qui permet de bâtir des réseaux sociaux pour des entités, jusqu'alors gratuit, a annoncé que le service deviendrait payant à compter du 1er juillet 2010. Abandonner un service au profit d'un autre est d'autant plus délicat pour celui qui a un historique de données et de contacts conséquent.

En outre, la fonction de recherche d'amis sur les réseaux sociaux (Facebook, MySpace, Twitter, LinkedIn, Netlog Friendster, Badoo, etc.) permet à partir d'un compte de voir si une adresse mél est rattachée à un utilisateur (prénom, nom). Contrairement à une adresse mél, le couple nom-prénom n'est pas considéré comme une donnée privée. On peut ainsi récupérer plusieurs millions de profils (adresse mél + nom + prénom + autres informations relatives au profil selon les préférences renseignées par l'utilisateur et le fait qu'il est ou non réglé ses paramètres de confidentialité de son compte) à partir d'une base de données d'adresses méls quelconques. Avec un générateur d'adresses mél aléatoires, ceci peut être automatisé et des captations d'informations sont possibles.



L'envoi de spams grâce aux adresses méls récoltées peuvent aussi comporter des programmes malveillants avec les liens et les pièces jointes comme ver, virus, sans compter le possible phishing qui a pour objet de frauduleusement récupérer les coordonnées bancaires d'un internaute.

Connaissant les souhaits d'un internaute, par exemple pour ses futures vacances, grâce aux informations glanées sur les réseaux sociaux, il est alors possible d'élaborer une offre de voyage correspondant à ses souhaits. En créant un faux site avec une proposition de billets d'avion à des prix imbattables (voire un séjour dans un hôtel, etc.), il est possible de lui adresser une offre *via* sa messagerie. La personne recevant cette offre conforme à ses aspirations sera incitée à cliquer vers une page infectée et des données personnelles y compris des coordonnées bancaires peuvent ainsi être indûment récupérées.

4. Les réseaux sociaux feront l'objet de plus en plus d'applications ayant recours à la **géolocalisation** du fait des connexions nomades *via* les PC portables reliés à Internet et les smartphones**.** Et outre le **fichage de la personne**, sa traçabilité sera mise en application faisant planer un risque de « bigbrotherisation ». Le principe du « *droit à la déconnexion* » pour ne pas être joint ou localisable lorsqu'on le souhaite risque d'être un privilège de classes aisées[1].

5. **L'utilisation des données** relatives à l'internaute, **en dehors de leur contexte ou de façon succincte ou dénaturée**, peut lui causer préjudice. En outre la persistance des données va à l'encontre du « *droit à l'oubli* » revendiqué par la CNIL. La difficulté est accrue par le fait que la plupart de ces outils sont Américains et les données qu'ils collectent hébergées à d'autres points du globe où la loi peut différer. Aussi les réponses législatives ne sont pas toujours applicables et les saisines des sites Américains quant à un préjudice subi relatif à l'identité numérique de l'internaute incertaines. De surcroît, les données, même effacées se heurtent à des obstacles techniques. Ainsi la machine de Wayback[2] ou du retour arrière permet d'avoir une image du web à une date donnée et de retrouver les traces d'informations

[1] Selon Umberto Eco dans l'une de ses nouvelles sur le téléphone mobile où il affirme que les seules personnes ayant du pouvoir dans le monde sont celles qui n'ont pas de téléphone portable et qui ne sont pas soumises aux appels incessants.

[2] Le site www.archive.org lui est associé.

passées publiées. Quant bien même des données seraient effacées, il est possible de les retrouver sans compter la possible duplication sur des kyrielles de sites, blogs et réseaux sociaux *via* par exemple la syndication de contenu (flux RSS).

Quelle conduite tenir pour utiliser les réseaux sociaux en se protégeant et en préservant ses libertés individuelles ?

En dépit de tous ces risques, il est légitime de se demander quelle est la conduite à tenir sur les réseaux sociaux. Ne pas être présent pourrait paraître comme suspect, comme si l'on avait rien à dire ou pire, des choses à cacher. Aussi la solution serait une utilisation intelligence des réseaux sociaux en les apprivoisant et en ayant conscience des risques pour mieux les maîtriser. Pour le bon usage des réseaux sociaux, 10 recommandations sont ainsi proposées :

1. Déterminer une stratégie pour votre présence sur le réseau social considéré (« *Pour quoi faire ?* », « *Quel est le bénéfice escompté ?* ») et s'assurer que l'image véhiculée est en phase avec cette stratégie.
2. Préalablement, avant toute inscription à un réseau social, lire la charte[3] d'utilisation du réseau social, la propriété des données publiées (textes, photos, vidéos) et les éventuelles sessions à des tiers, etc. Paramétrer son profil pour décider quelles informations personnelles vous souhaitez afficher (auprès de vos amis, des amis de vos amis, des autres utilisateurs du réseau social).
3. Sélectionner ses amis et importer des contacts *via* ses messageries et ne pas accepter de demande d'amis sans les connaître préalablement et vérifier le cas échéant les identités *via* les adresses méls connues ou en contactant préalablement la personne pour s'assurer qu'il est bien celle qu'elle prétend être. Opter pour plusieurs adresses mél sur les réseaux sociaux pour prévenir le risque de spam.
4. Créer des groupes sélectifs dans différentes sphères : travail, famille, amis, etc. Et segmenter son activité.
5. Renseigner son profil en étant vigilant en ce qui concerne les informations sensibles qu'il convient de communiquer en connaissance de cause.
6. Réciproquement, faire des liens depuis son site/blog vers ses réseaux sociaux dans une optique de développement d'audience (si cet objectif est recherché).
7. Veiller aux informations communiquées, en particulier celles relatives à la vie privée.
8. Créer plusieurs profils si nécessaire pour séparer le cas échéant son identité professionnelle de son identité privée.
9. Mettre à jour votre statut en fonction de la stratégie poursuivie.
10. Participer à des groupes de discussion selon ses intérêts et ses objectifs en étant également vigilant.

---

[3] Celle-ci peut évoluer dans le temps. Ainsi les informations qui figurent sur Facebook sont propriété de Facebook y compris le contenu que l'on publie. L'article deux de la *Déclaration des droits et responsabilités* indique que pour le contenu protégé par les droits de propriété intellectuelle, l'abonné accorde une licence non-exclusive, transférable, sous-licenciable, sans redevance et mondiale pour l'utilisation des contenus de propriété intellectuelle qu'il publie sur Facebook. Facebook a ainsi la permission de donner le droit à n'importe qui d'exploiter les photos, vidéos, textes et autre contenu qui figurent sur son compte. Cette licence se termine lors de la fermeture définitive du compte, mais des fichiers peuvent être conservés dans les copies de sauvegarde. En outre, étant donné que la licence est sous-licenciable, des tiers peuvent avoir obtenu le droit de diffuser des éléments avant la fermeture de votre compte.

Dans ce contexte, il devient important de surveiller son identité numérique, ce que l'on appelle le « *Personal branding* ». Cette activité de veille est facile à mettre en œuvre en s'abonnant à des alertes relatives à son identité sur Google[4] et Twitter principalement (prénom + nom, initiale du prénom + nom, etc.) et en utilisant des outils comme 123 People ou WebMii. Si des informations communiquées par des tiers sont erronées ou portent atteinte à la vie privée ou à l'image, il est important d'apporter un démenti ou des précisions le plus rapidement possible, avant que le contenu soit lu (et repris sur d'autres outils su web 2.0) par un nombre croissant d'internautes.

Il est également possible de choisir les réseaux sociaux sur lesquels on souhaite s'inscrire et collaborer même si la pression de ses contacts conduit à opter pour les outils massivement diffusés comme Facebook. Il existe également des réseaux sociaux dont la gestion des données est décentralisée (souvent c'est l'internaute lui-même qui héberge ses données personnelles). Encore peu répandus aujourd'hui, des initiatives sont à noter comme Diaspora ou Movim. Ce pourrait être une piste plus sûre pour la protection des données personnelles.

Il est difficile d'empêcher que des informations fournies dans un contexte soient réutilisées à l'insu de leur propriétaire. Tout au plus, il est possible d'exercer un droit d'accès *a posteriori* en contactant la personne les ayant publiées et en lui demandant amiablement d'apporter des rectifications ou précisions. Notons que des sociétés sont spécialisées quant à l'image numérique d'une personne. Elles peuvent intervenir de façon onéreuse pour demander à ce que des informations qui causent préjudice à un internaute soient effacées. Et elles peuvent également publier des informations positives sur la personne de façon à ce que les informations qui causent du tort n'apparaissent plus dans les premières positions délivrées par les moteurs de recherche, Google en tête, et soient ainsi reléguées plus loin.

Par ailleurs, contraindre les fournisseurs de services à adopter une pratique respectueuse des libertés, du droit à la vie privée et à l'oubli n'est pas une démarche aisée. Et l'apparente gratuité des outils doit faire redoubler de vigilance. Néanmoins, chaque internaute peut choisir les réseaux sociaux qui lui semblent le plus éthiques possible dans la gestion des données personnelles. Ce pourrait être une carte à jouer pour les réseaux sociaux décentralisées qui commencent à apparaître Enfin, contrairement aux États-Unis, la France a été marquée par la Collaboration et le rapport aux données n'est pas le même (le principe de l'opt-in prévaut).

Les réseaux sociaux transforment notre façon de penser, d'agir et notre rapport au temps, à l'espace et à autrui. Aussi il devient plus que nécessaire d'être vigilant et d'agir avec discernement pour préserver nos libertés individuelles.

David Fayon

Auteur de « ***Web 2.0 et au-delà*** », Économica, 2e édition, 2010 et de « ***Facebook, Twitter et les autres…*** » (avec Christine Balagué), Pearson, 2010, anime le Portail Internet et NTIC (http://david.fayon.free.fr)

Sources et pour aller plus loin :

[4] www.google.fr/alerts?hl=fr

Réseaux sociaux et structures relationnelles, Emmanuel Lazega, Puf, Que sais-je ?, 2007

Sociologie des réseaux sociaux, Pierre Mercklé, La Découverte, 2004

Facebook, Twitter et les autres…, Christine Balagué, David Fayon, Pearson, 2010