# LES RESEAUX SOCIAUX ET LA QUESTION DES LIBERTES INDIVIDUELLES

Cette année, le pôle TICE académique dans le cadre de sa mission d'information et de conseil a décidé de s'intéresser au phénomène des réseaux sociaux et messageries instantanées. Nous essayerons de vous transmettre des informations vous permettant de sensibiliser vos élèves aux bonnes pratiques d'utilisation de ces nouveaux outils de communication afin qu'ils évitent toutes dérives et soient des acteurs responsables et informés des usages numériques.

## 1) PRINCIPE DES RESEAUX SOCIAUX SUR INTERNET

Il s'agit d'un ensemble d'identités sociales, telles que des individus ou organisations sociales, reliées entre elles par des liens créés lors de relations privilégiées.

Il s'agit souvent d'une structure sociale dynamique qui se modélise par des sommets et des arrêtes, les sommets étant généralement des gens et/ou des organisations reliés entre eux par des interactions sociales.

La notion de « médias sociaux » recouvre alors ces activités en y intégrant la technologie et la création de contenu.

Andreas Kaplan et Michael Haenlein définissent les médias sociaux comme « un groupe d'applications en ligne qui se fonde sur la philosophie et la technologie du web 2.0 et permet la création et l'échange du contenu généré par les utilisateurs »[1].

Aujourd'hui, de par l'explosion de l'utilisation des outils numériques et la généralisation de l'internet, de nombreux réseaux s'offrent à différents utilisateurs.

Certains regroupent des amis de la vie réelle, tel Copains d'avant, d'autres aident à se créer un cercle d'amis, à trouver des partenaires commerciaux, un emploi ou autres. Il s'agit de services de réseautage social comme Facebook, MySpace, Trombi.com, Twitter, Google Buzz, Linkedln, FlickR...

## 1) QUELQUES EXEMPLES DE RESEAUX SOCIAUX

**Facebook** : premier réseau social, 500 millions d'utilisateurs dans le monde. En France, 20 millions.

L'inscription est extrêmement simplifiée, l'âge limite fixé à 13 ans (en théorie).

On crée un profil en renseignant (ou pas) des informations personnelles et ainsi on partage son statut avec des amis qu'on sollicite grâce à leur nom ou adresse mél.

**Twitter** : Presque un mini blog. On y écrit son actualité en direct. Gros avantage, la possibilité d'envoyer des messages de 140 signes (tweets).

Des « followers » ou abonnés à votre compte peuvent alors vous suivre au quotidien. Publication très rapide.

**FlickR** : Créer en 2004. Réseau social de photos. Il regroupe des professionnels mais aussi des amateurs en recherche de notoriété. Portefolio et base de données de photos libres de droits y sont disponibles.

**MySpace** : Un des réseaux les plus importants. Bien spécifique pour la musique, les vidéos.

**Des nouveautés :**

**Foursquare et Gowalla** : réseaux de géolocalisation. Vous avez un compte personnel, naturellement relié à d'autres personnes. Lorsque vous vous trouvez dans un endroit, vous signalez votre présence à votre réseau qui instantanément peut alors vous géolocaliser.

Le « Check in » peut également permettre de signaler une enseigne commerciale où vous vous trouvez et vous permettre de gagner des points de réduction ou encore de devenir « Maire » virtuel d'un lieu.

Cette liste de réseaux sociaux est loin d'être exhaustive. Pour autant, au-delà de leur utilité avérée, ces nouveaux outils de communication comportent des risques en matière de protection de la vie personnelle.

La publication de contenus souvent personnels sur les blogs et les réseaux sociaux, les chats et autres sont désormais entrés dans le quotidien de tous, ceci sans qu'aucun garde fou ne soit fixé. A travers ces usages, la ligne de partage entre vie privée et vie publique tend à se dissiper.

## 3) QUELS RISQUES COURONS-NOUS DANS CES NOUVELLES PRATIQUES ?

1. **L'usurpation d'identité existe**. Il est facile d'endosser l'identité d'un tiers en collectant par exemple sa photo sur le web. Connaissant quelques informations de nature personnelle (date de naissance, profession) un internaute mal intentionné peut alors créer un faux profil sur le réseau social, entrer en contact avec les personnes susceptibles de connaître la personne incarnée.

   En cas de fraude, c'est souvent à la vraie personne d'apporter la preuve qu'elle est bien la bonne personne. L'usurpation d'identité sur internet longtemps non condamnée du fait d'un vide juridique semble –t-il le sera dans le cadre de la loi LOPPSI 2.

2. **Le piratage des données**. Des données stockées peuvent être indûment copiées, modifiées, effacées, vendues à des tiers. L'interaction entre les réseaux sociaux facilite ces piratages. Le risque est alors l'utilisation de ces données à des fins malveillantes, publicités non sollicitées. Mais un scénario catastrophe serait l'utilisation de ces données par un gouvernement autoritaire qui ségréguerait des catégories de citoyens en utilisant les informations renseignées par les internautes eux-mêmes. Attention au mot de passe qui peut être récupéré et utilisé pour prendre contrôle de votre compte et y ajouter des éléments graves pour votre réputation.

3. **Les données collectées utilisées à des fins commerciales ou autres**. Le module Beacon de Facebook qui a suscité un tollé de la part des internautes et des abonnées car il informait les amis des utilisateurs quand ceux-ci visitaient un site internet affilié. Facebook sous la pression a dû modifier cette fonction. Cependant, sachant que les conditions d'utilisation d'un outil peuvent changer dans le temps, la vigilance est de rigueur.

   Autre vigilance, la fonction « recherche d'amis » sur les réseaux sociaux (Facebook, MySpace,Twitter, 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 ait ou non réglé les paramètres de confidentialité de son compte) à partir d'une base de données d'adresses méls quelconques.

C'est ainsi que l'envoi d'un spam (Le **spam**, **pourriel** ou **polluriel** est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.) grâce aux adresses méls récoltées, peut aussi comporter des programmes malveillants avec des liens et les pièces jointes comme ver, virus, sans compter le possible **phishing** (piratage de lignes) qui peut avoir pour objet de récupérer frauduleusement les coordonnées bancaires d'un internaute.

4. **Les dangers de la géolocalisation**. De plus en plus d'applications ont recours à la géolocalisation du fait des connexions nomades *via* les PC portables reliés à Internet et les smartphones. La traçabilité et le fichage de la personne semblent être le futur, faisant planer le risque de la « 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[2].

5. L'utilisation des données relatives à l'internaute, en dehors de leur contexte ou de façon succincte ou dénaturée, peut lui causer préjudice. Malgré les rappels de la CNIL, le « droit à l'oubli » est loin d'être une réalité, d'autant plus que la plupart de ces outils sont Américains et les données qu'ils collectent hébergées à d'autres coins de la planète où les lois peuvent différer.
6. Les données même effacées se heurtent à des obstacles techniques. Ainsi, la machine de « Wayback »[3] ou du « retour arrière » permet d'avoir une image du web à une date donnée et de retrouver les traces d'informations anciennement publiées. Quand bien même les 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).

# 4) QUELLE CONDUITE TENIR POUR UTILISER LES RESEAUX SOCIAUX EN PRESERVANT SES LIBERTES INDIVIDUELLES ?

En dépit de tous ces risques, l'usage des réseaux est possible si on adopte une utilisation intelligente, en ayant conscience des risques pour mieux les maitriser.

1. Déterminer une stratégie de présence sur le réseau social : « Pour quoi faire ? », « Quel est le bénéfice escompté ? » faire attention à l'image véhiculée qui doit être en phase avec la stratégie définie.
2. Avant toute inscription à un réseau social, lire la charte d'utilisation, 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. Bien sélectionner ses amis, importer des contacts via ses messageries et ne pas accepter de demande d'amis sans les connaître préalablement. Vérifier les adresses méls via les adresses connues ou en contactant la personne pour s'assurer qu'elle est bien celle qu'elle prétend être. Opter pour plusieurs adresses méls 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 c'est un objectif 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 et 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.

## 5) SURVEILLER SON IDENTITE NUMERIQUE

Certains outils vous permettent de surveiller votre identité numérique, ils sont appelés ***« Personal branding »***. Cette activité de veille est facilitée en s'abonnant à des alertes relatives à son identité sur Google 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 possible alors d'apporter un démenti ou des précisions le plus rapidement possible, avant que le contenu ne soit lu ou repris sur le web2.0 par des nombres croissants d'internautes.

Autre solution, choisir les réseaux sur lesquels on souhaite s'inscrire et collaborer en résistant à la pression de ses contacts qui souvent conduit à opter massivement pour les réseaux les plus utilisés.

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).

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

W. Tchamaha

Sources :

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

---

[1] Kaplan Andreas M., Haenlein Michael (2009) *Utilisation et potentiel commercial des hyperréalités : une analyse qualitative de Second Life*, Revue Française du Marketing, N°222, 69-81.

[2] Selon Umberto Eco dans 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.

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