

# Vie privée sur internet

Et Rôle des réseaux sociaux dans le commerce électronique (e-commerce)

Mohammed ALAMI MEJJATI

## **Table des matières**

### **I. Introduction**

### **II. Généralités sur la vie privée**

### **III. Définition des réseaux sociaux**

### **IV. Tour d’horizon de 5 réseaux sociaux**

#### **IV.1 Définition et historique**

#### **IV.2 Politiques en matière de vie privée**

#### **IV.3 Modèles économiques**

### **V. Développements et technologie**

#### **V.1 Moyens technologiques**

#### **V.2 Fonctionnalités**

#### **V.3 Perspectives**

### **VI. Risques pour l’individu et l’entreprise**

#### **VI.1 Vols d’identité**

##### **VI.1.a Problématique et exemples réels**

##### **VI.1.b Solutions proposées**

#### **VI.2 Vente de profils de consommation**

#### **VI.3 Constitution de dossiers sur les personnes**

#### **VI.4 Monitoring des salariés**

#### **VI.5 E-réputation de l’entreprise**

### **VII. Usage des médias sociaux pour l’entreprise**

#### **VII.1 Marketing viral**

#### **VII.2 Lancement de produits et branding**

#### **VII.3 Développement d’e-commerces**

### **VIII. Conclusion**

## **I. Introduction**

Glenn CHAPMAN de l'AFP rapportait dans son article célébrant les quarante années d'Internet "Il y a quarante ans, Leonard Kleinrock était loin d'imaginer que des phénomènes de société planétaires comme Facebook, Twitter ou Youtube découleraient de l'invention à laquelle il venait de donner naissance avec son équipe : internet"<sup>1</sup>.

Mais un tel développement des réseaux sociaux ne va pas sans poser des problèmes d'ajustement et de besoin de normalisation des moyens de protection des données dans l'espace virtuel pour correspondre à nos standards et acquis de la vie réelle. En effet, concernant les droits accordés aux individus en matière de vie privée, qui sont exprimés dans la Déclaration universelle des droits de l'homme de 1948, et, pour l'Europe, par la Convention européenne qui en reprend les grands principes, ne peuvent être sacrifiés ou mis en péril par l'avènement d'une technologie quelconque.

Or, ces réseaux qui bâtissent leur stratégie sur la collecte d'informations de tout genre, ne disposent pas toujours de règles de protection en matière de vie privée adaptées, traitent souvent avec des tierces parties pour le développement d'applications qui viennent enrichir leurs plateformes et donc peuvent engendrer la fuite de données personnelles des individus, et font l'objet d'attaques qui révèlent la fragilité de leurs infrastructures.

Dés lors, on est en droit de se poser des questions quant à leurs valeurs et politiques.

D'autre part, avec des taux de progression à trois chiffres pour certains sites, des créations de listes orientées business de manière inopinée, et une utilisation accrue dans la stratégie marketing e-business, y compris par les grosses entreprises, les réseaux sociaux s'imposent comme un canal média incontournable dans l'industrie de l'internet.

Aussi, nous allons analyser les problèmes posés par ces réseaux concernant la protection de la vie privée, définir les enjeux importants pour cerner notre champ de recherche, étudier des cas réels de fraude survenus, et tenter d'y apporter des solutions concrètes.

## **II. Généralités sur la vie privée**

La vente en ligne pose la question de vie privée, du fait de la nécessité d'un nombre important d'informations pour conclure une transaction électronique. Il est donc légitime pour le consommateur de se préoccuper de l'utilisation de ces données personnelles. Le respect de la vie privée d'un point de vue de droit consiste à empêcher la divulgation de celles-ci en accordant à l'individu le contrôle de ses informations. Ce concept porte sur le

droit à l'information (renseignements collectés), le droit de consentement (refuser éventuellement la collecte), droit de contrôle de l'utilisation qui en est faite (intrusions non souhaitées) et le droit d'accès et correction des informations erronées.

Si l'informatisation des données a été généralement considérée comme un progrès, elle s'est accompagnée de peurs, voire de fantasmes nourris par « Big Brother », au sujet de la possibilité pour autrui ou pour un pouvoir institué, de tout connaître d'un individu.

Internet a amplifié cette peur puisque désormais les ordinateurs communiquent entre eux.

Si le droit à la vie privée est bien protégé par des lois avec au Canada la LPDRE (la Loi sur la Protection des renseignements personnels), en Europe avec la Directive 95/46/CE, aux états unis elle est simplement objet de principes nommés « Safe Harbour Privacy Principles » issus directement de la Directive européenne mais agissant en simple label<sup>2</sup>.

Pour rappel, au Canada on définit un renseignement personnel tout renseignement qui concerne une personne physique et permet de l'identifier (adresse IP, login, courriel...etc.)

### **III. Définition de réseau social (social network)**

On peut le définir comme suit « Communauté d'individus ou d'organisations en relation directe ou indirecte, rassemblée en fonction de centres d'intérêts communs, comme par exemple les goûts musicaux, les passions ou encore la vie professionnelle. »<sup>3</sup>.

Toutefois on distingue 2 catégories : à usage professionnel ou destiné au grand public.

Si en effet le premier réseau d'AOL date de 1988, ce n'est qu'en 1998 que "SixDegrees" est né et la progression va rester relativement lente pour s'accélérer en 2006 (vote de la loi 410-15 aux USA pour interdire les réseaux sociaux aux mineurs<sup>4</sup>) avec domination de Facebook<sup>5</sup> jusque 2008 où il détrôna Myspace du premier rang et on verra Twitter<sup>6</sup> passer du 22ème rang au 3ème avec en prime l'élection de Barack Obama, candidat des réseaux sociaux sur Internet<sup>7</sup> et le changement des réseaux en médias. 2009 verra la consécration de Twitter (Nielsen a reporté que Twitter enregistrerait 21 millions de visiteurs uniques soit une croissance de 2000% par rapport à 2008. Dans son rapport "Social Network Site Privacy : A Comparative Analysis of Six Sites"<sup>8</sup>, J.Barrigar parle de "social network site" vs "social networking sites.". Mais les réseaux sociaux sont devenus des médias sociaux, puisqu'on a placé de la publicité sur des plateformes qui servent à créer des relations, et qui ne sont pas à proprement parler des supports de contenu. Citons enfin Fred Cavazza<sup>9</sup> qui en dresse un panorama satisfaisant.

## IV. Tour d'horizon de 5 réseaux sociaux

Pour mon étude j'ai pris les trois réseaux sociaux grand public figurant au palmarès des plus populaires en février 2009 selon Compete.com<sup>6</sup>. Les grands gagnants de cette liste sont l'incontournable **Facebook**, **Myspace**, le percutant **Twitter** (1 Américain sur 10 est désormais sur Twitter) et les réseaux s'adressant à des audiences de niche tels que **LinkedIn** et **Viadeo** son concurrent en Europe (réseaux destinés aux professionnels).

LinkedIn figure toutefois au palmarès TOP 25 de Compete.com puisqu'il est classé 5ème.

### IV.1 Définition et historique

**Facebook** se définit comme un réseau social qui aide les gens à communiquer plus efficacement avec leurs amis, familles et collègues de travail<sup>8</sup>. Né à Harvard en 2004, initialement destiné à rassembler les lycéens et étudiants des pays anglophones. Depuis 2007, le site est ouvert à tous. Une fois inscrit gratuitement, les utilisateurs doivent compléter leur profil en donnant des informations liées à leur état-civil, leurs centres d'intérêt etc. La particularité de Facebook est la possibilité offerte à ses utilisateurs d'ajouter sur leur profil des fonctionnalités (applications) développées par des tiers.

**Myspace** vise principalement les jeunes, leur donnant la possibilité de s'exprimer librement et d'entretenir des rapports avec les marques et les groupes de musique.

En 2002, plusieurs employés d'eUniverse disposant d'un compte Friendster ont réalisé son potentiel et ont décidé de l'imiter. MySpace a été lancée en 2003 comme site communautaire avant de devenir indépendant en Janvier 2004, puis vendu à NewsCorp en Juillet 2005, pour faire partie de la division de Fox Interactive Media (Cie Murdoch).

Le succès de Myspace est attribué à la possibilité de personnaliser les pages de profil<sup>10</sup>.

**Twitter** quant à lui est un réseau social de microblogging, permettant aux utilisateurs de bloguer grâce à des messages courts (140 caractères maximum, soit une ou deux phrases) mais sans possibilité de commenter les messages postés. Selon son slogan, Twitter permet de raconter ce qu'on fait au moment où on le fait, mais en pratique les utilisateurs l'utilisent plutôt pour s'échanger des informations et des liens. Le principal facteur de son succès réside dans son respect absolu du principe « Keep it Simple, Stupid »<sup>11</sup>.

Twitter a été créé à San Francisco par Evan Williams et Noah Glass. Ce dernier, ancien répartiteur au 911, avec Jack Dorsey dispatcheur pour une compagnie de taxis, furent chargés de développer un nouveau service. L'idée de départ était de permettre aux

utilisateurs de décrire ce qu'ils étaient en train de faire via SMS. Ouvert au public le 13 juillet 2006, la première version s'intitulait stat.us puis twittr. En avril 2007, une entité indépendante est créée portant le nom de Twitter, Inc. avec Jack Dorsey à sa tête jusqu'en octobre 2008 date à laquelle Evan Williams lui succédera<sup>12</sup>. En Juin 2009 Nielsen a reporté que twitter enregistrait une croissance de 1444% par rapport à l'année dernière<sup>13</sup>.

**LinkedIn**, dans la catégorie des réseaux sociaux à usage professionnel, «a pour objet de fournir un service pour faciliter le réseautage professionnel entre les Utilisateurs partout dans le monde. Le site est destiné à permettre aux Utilisateurs à se connecter uniquement à d'autres Utilisateurs qu'ils connaissent au moment de la connexion et à approfondir leurs relations professionnelles avec ces Utilisateurs.»<sup>14</sup>. LinkedIn offre un moyen efficace par lequel les gens peuvent développer une longue liste de contacts, en tant que tel votre réseau est constitué de vos propres connexions, les connexions de vos connexions (2ème degré), en plus des connexions de votre 2ème degré (3ème degré). Ainsi R.Gervais, PDG de Zerofail à Montréal dispose d'une liste de 1 494 800 contacts<sup>15</sup>. LinkedIn a été fondée en Mai 2003, «lorsque les cinq fondateurs ont invité 300 de leurs contacts les plus importants à y adhérer». Un mois après, le site comptait déjà 4500 membres, et après un an de son lancement, le site comptait plus de 500.000 membres. En Mai 2009, LinkedIn fête son 6ème anniversaire avec 40 millions de membres<sup>16</sup>.

**Viadeo** pour sa part, est présent sur les cinq continents, et offre à plus de 25 millions de professionnels des solutions pour développer leur réseau et opportunités d'affaires tant à l'échelle locale que globale. Basée à Paris, la société dispose de bureaux en Angleterre (Londres), en Espagne (Madrid et Barcelone), ainsi qu'en Italie (Milan). Viadeo est également présent sur le continent américain grâce à ses filiales mexicaine et canadienne. Le groupe est par ailleurs fortement implanté sur le marché asiatique en Chine et en Inde. Viadeo est un réseau social professionnel créé par Dan Serfaty et Thierry Lunati, apparu sur la toile en mai 2004, sous le nom de Viaduc, puis appelé Viadeo en novembre 2006<sup>17</sup>. Viadeo se différencie fondamentalement des autres réseaux, pour avoir concentré ses services de qualité pour les professionnels et les entreprises qui peuvent l'utiliser pour stimuler leur carrière et la croissance de leurs business, le tout en six langues. Viadeo reste fidèle à son positionnement stratégique, contrairement à LinkedIn qui vient de s'ouvrir au microblogging en intégrant les tweets des profils ayant un compte Twitter<sup>18</sup>.

## IV.2 Politiques en matière de vie privée

**Facebook** détient une licence certifiée du programme de confidentialité TRUSTe Privacy Seal Program. TRUSTe, est une organisation indépendante spécialisée dans le contrôle des politiques et pratiques de sécurité et de confidentialité. Facebook adhère également au programme «Safe Harbor framework» proposé par le Département américain du Commerce et par l'Union européenne<sup>19</sup>. Toutefois il est souvent objet de critiques pour manque de transparence comme l'affaire Beacon<sup>20</sup> en 2007, la suppression des données<sup>21</sup> en 2008, et récemment les critiques du commissaire à la vie privée du Canada qui l'ont obligé à proposer une nouvelle version de politique de confidentialité<sup>22</sup> fin Octobre 2009. Dans la politique de Confidentialité de **Myspace** en vigueur depuis Février 2008, il y est fait mention de « l'IPI » informations personnellement identifiables nom et prénom, adresse électronique, adresse postale, numéro de téléphone ou numéro de carte de crédit. La collecte et l'utilisation de ces 'IPI' sont détaillées sans toutefois faire référence à une norme quelconque<sup>23</sup>. Cela paraît normal dans la mesure où 70% de l'audience se trouve aux USA contrairement à Facebook où plus de 70% des utilisateurs sont hors USA<sup>8</sup>. Quant à **Twitter**, sa politique est claire, concise et propre à son utilisation. Ainsi on voit une clause concernant le lieu puisque le site offre plusieurs services de proximité<sup>24</sup>. **LinkedIn** s'aligne sur Facebook et indique dans sa Politique de confidentialité qu'il participe à l'EU « Safe Harbor Privacy Framework » et est certifié pour répondre aux normes de confidentialité strictes de l'Union européenne. Toutes les relations sont mutuellement confirmées. Il fait partie du programme de confidentialité TRUSTe<sup>25</sup>. L'âge minimum pour son utilisation fixé à 18ans le différencie des autres cités (13ans). Dans **Viadeo**, bien que la confidentialité des données fasse simplement l'objet d'un article au sein des termes d'utilisation, assez court, il est stipulé que le site a fait l'objet d'une déclaration auprès de l'autorité française de protection des données personnelles (la Commission Nationale de l'Informatique et des Libertés - CNIL). Il est stipulé clairement « Vous disposez d'un droit d'accès, de rectification et de suppression des données qui vous concernent (art. 34 de la loi relative à l'informatique, aux fichiers et aux libertés)»<sup>26</sup>. De ce qui précède, nous pouvons déjà relever certains points, comme par exemple l'effet label de confiance (TRUSTe en l'occurrence) ainsi que l'importance des lois nationales dans le cas de Viadeo par opposition à un simple consensus tel que Safe Harbor Privacy.

### IV.3 Modèles économiques

Pour les deux réseaux en tête, **Facebook** et **Myspace** : le business model reste celui de la publicité. Les 2 leaders monétisent leur audience, plus quelques spécificités propres à leur public. Myspace music procure une autre source de revenu à Myspace avec ses ventes de musique en ligne en plus des deals publicitaires de plusieurs millions<sup>27</sup>. **Facebook** de son côté essaie de trouver d'autres sources de revenus comme avec les cadeaux virtuels; des crédits que les utilisateurs peuvent se donner entre eux. Concernant **Twitter**, la publicité n'est pas à l'ordre du jour. Selon le co-fondateur de Twitter, Biz STONE, le site cherche à développer de nouveaux outils, allant de l'amélioration de la recherche à des fonctionnalités payantes pour les comptes commerciaux<sup>28</sup>.

Pour les réseaux sociaux professionnels, Les 2 acteurs s'appuient sur le même business model qui se décline en 3 sources de revenus : Les abonnements de membres, Les offres d'emploi et La publicité sur le site. Pour **LinkedIn**, les ratios du CA sont comme suit : La publicité sur le site 25 %, les abonnements de membres 60 % et les offres d'emploi représentent 15 %. **Viadeo** annonce que 50% de ces revenus provient des abonnements et 50% du pôle Job/Publicité/Formation<sup>29</sup>.

Il en ressort que si les réseaux sociaux drainent beaucoup de trafic, ils cherchent encore leur business modèle. **Facebook** et **Twitter** ne sont pas encore rentables.

En revanche les réseaux sociaux professionnels sont rentables. Une grande part de cette rentabilité provient des abonnements que paient les utilisateurs, ce qui fait leur force.

## V. Développements et technologie

### V.1 Moyens technologiques

Les réseaux sociaux se sont développés avec le « WEB 2.0 », terme souvent utilisé pour désigner ce qui est perçu comme une transition importante du World Wide Web, passant d'une collection de sites Web à une plate-forme informatique à part entière, fournissant des applications Web aux utilisateurs. Plus qu'une technologie c'est en fait un concept de mise en commun d'informations.»<sup>30</sup>. C'est ainsi que les réseaux sociaux favorisent l'intelligence collective. *Stricto sensu*, l'intelligence collective est un concept régulateur qui peut être défini comme une intelligence variée, partout distribuée, sans cesse valorisée, coordonnée en temps réel, qui aboutit à une mobilisation effective des compétences<sup>31</sup>. En 2006 en comptait déjà plus d'1 milliards d'internautes. La révolution

est que chacun peut alimenter le contenu d'Internet et ainsi proposer de nouveaux socles de connaissances. De la sorte, les réseaux sociaux partagent avec le «Web 2.0» son socle technologique, où il s'agit d'une évolution des usages faits des technologies existantes.

a) XML : Ce langage de balisage (XML signifie eXtensible Markup Language ou langage de balisage extensible) est à la base de nombreux langages sur le web pour son côté extensible. Plusieurs flux d'informations sont émis par les sites web sous ce format.

b) XHTML : langage de balisage suit le HTML pour les pages web. XHTML signifie eXtensible Hyper Text Markup Language (langage de balisage hypertexte extensible).

c) CSS : Les Cascade Style Sheets (feuilles de style en cascade) permettent de définir la présentation des pages XHTML et HTML et séparer un contenu de sa présentation.

d) Javascript : Ce langage de script permet de manipuler et de modifier dynamiquement des pages XHTML et HTML sur le poste du client. Aussi utilisé pour les contrôles.

e) AJAX : permet de mettre à jour des éléments d'une page web sans avoir à la rafraichir dans son ensemble. Une application web classique fonctionne de manière synchrone, une application web avec AJAX permet de recharger certains éléments particuliers de la page de manière transparente, sans recharger la page entière. Ceci améliore le confort de l'utilisateur et lui permet de gagner en interaction.

f) RSS et Atom : RSS signifie Really Simple Syndication : fichier XML mis à jour en temps réel. Il reprend automatiquement soit les titres, soit le texte intégral, d'un site d'actualité ou d'un blog. Atom est juste une autre technologie pour le même résultat.

g) ReST : ReST est un terme inventé par Roy Fielding dans son mémoire Ph.D en 2000, pour décrire un style d'architecture des systèmes en réseau. ReST est l'acronyme de Representational State Transfer. Le Web est composé de ressources. Une ressource est un objet d'intérêt. Ainsi, le Boeing Aircraft Corp peut définir une ressource 747. Les Clients peuvent y accéder alors avec l'URL : <http://www.boeing.com/aircraft/747><sup>32</sup>.

## **V.2 Fonctionnalités**

Les réseaux sociaux intègrent des aspects fonctionnels qui sont aujourd'hui banalisés :

a) Blogging : une publication fréquente de pensées personnelles, séquentielle, temporelle.

b) Widgets : petite application ou contenu dynamique aisément inséré dans une page web.

c) Mashups : utilisation par une application ou un service d'un ou de plusieurs autres

services disponibles en ligne, l'ensemble apparaissant comme une application originale et cohérente. Il est le résultat de la combinaison de plusieurs sources/applications existantes.

d) Wikis : Un wiki est un logiciel de la famille des systèmes de gestion de contenu de site web rendant les pages web modifiables par tous les visiteurs y étant autorisés<sup>33</sup>.

e) Tags : Le tag est une étiquette attribuée à un contenu pour le caractériser, nuage de tags

f) SaaS : Le logiciel en tant que service (Software as a Service) est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence. Il n'y a alors plus besoin d'installer une application de bureau ou client-serveur. Ce concept, apparu au début des années 2000, prend la suite du fournisseur de service d'application « ASP »<sup>34</sup>.

### V.3 Perspectives

Plusieurs recherches sont faites dans ce sens, et des scénarios sont imaginés pour intégrer ces réseaux sociaux dans le monde économique, pour qu'ils deviennent des acteurs incontournables de notre société (tel le principe de « Google AdSense » avec des micros paiements simples pour les contributions aux réseaux, ou encore la voie du e-commerce, en tant qu'apporteur de nouveaux clients à une marque, ils bénéficieraient de leur trafic).

En 2010, les médias sociaux seront encore plus populaires, plus mobiles, et plus exclusifs. Quelles sont les tendances à court terme, à voir dès l'an prochain<sup>35</sup> ?

1. Les médias sociaux commencent à se détacher de leur étiquette sociale : avec des groupes, des listes et des réseaux de niche de plus en plus populaires (listes Twitter).
2. Les entreprises auront une politique de médias sociaux : elles devraient formaliser la façon dont elle les perçoit et de la participation de ses employés à ces médias.
3. Le mobile, l'avenir pour le media social : avec environ 70 pour cent des sociétés qui interdisent l'utilisation des réseaux sociaux et, les ventes de Smartphones en hausse, il est probable que les employés aient recours à leurs appareils mobiles pour rester 'connectés'.
4. Nouvelles technologies et nouvelles fonctionnalités : Google Wave donne le ton. C'est un condensé de ce qui a fait le succès d'internet (messagerie instantanée, Skype et vidéoconférences, échange de photos à la Picasa, Doodle et sondages, Réseau social à la Twitter...). Google Wave se veut être plus complexe que le réseau social Facebook<sup>36</sup>.
5. Les réseaux sociaux devraient intégrer la géo localisation : pont entre le réseautage social et l'interaction sociale réelle, on voit déjà des signes précoces avec des services comme Foursquare, Gowalla, loopt, Brightkite, et Google Latitude<sup>37</sup>, à divers degrés.

## **VI. Risques pour l'individu et l'entreprise**

### **VI.1 Vols d'identité**

#### **VI.1.a Problématique et exemples réels**

Comme tout ce qui est nouveau, des problèmes et des imprévus se présenteront à l'utilisation de ces nouvelles technologies. En mai 2009, la France touchée par le phénomène d'usurpation d'identité avec plus de 210.000 victimes par an comme rapporté par le Figaro<sup>38</sup>, connut un projet de loi dit LOPPSI (loi d'orientation et de programmation pour la performance de la sécurité intérieure)<sup>39</sup> qui sanctionne l'usurpation d'identité en ligne. En juin 2009, le périodique des professionnels anglophones de la sécurité informatique «CSO»<sup>40</sup> publiait un article consacré aux 7 péchés capitaux de la sécurité sur les sites de réseautage social. En Juillet 2009, le site officiel de l'ISIQ (Institut de sécurité de l'information du Québec) publiait un commentaire fort engagé concernant un article de La Presse Affaires où il pose la question « Mais est-ce nécessaire de déboursier un certain montant tous les mois pour obtenir une protection efficace contre le vol d'identité ? ». Il définit en outre le vol d'identité comme suit « Le vol d'identité survient lorsqu'une personne prend possession de vos renseignements personnels sans vous avertir ou sans demander votre permission, généralement en vue de commettre un crime comme une fraude ou un vol »<sup>41</sup>. En Septembre 2009, on pouvait lire sur le site de Canoë.ca<sup>42</sup> que Guy Laliberté était victime d'usurpation d'identité. Il réclamait 1,5 M\$ à l'auteur et à l'éditeur de sa biographie non autorisée, qu'il accuse d'avoir emprunté son identité pour créer une page sur MySpace et pour opérer un blogue à son nom. Début Octobre 2009, c'est le directeur du FBI en personne qui a failli communiquer ses coordonnées bancaires à un site d'hameçonnage, avant de s'en rendre compte. Il en fait l'aveu sur le site officiel du FBI<sup>43</sup>, où il parle des menaces sur Internet concernant le vol d'identité et la cybercriminalité. Selon ses propos «Internet n'est pas seulement un canal pour le commerce, mais aussi un canal pour le crime.». Pour rappel, le mois d'Octobre est le mois de sensibilisation à la cybersécurité au Canada et aux États-Unis. Placée sous le thème de la responsabilité partagée, la campagne américaine, visait à inciter le plus grand nombre d'entreprises, d'organismes et d'individus à passer à l'action, à endosser ou à éduquer autour d'eux. Le sénat américain a adopté la résolution 285 en appui à la campagne nationale de sensibilisation à la sécurité de l'information. Au Canada, la

campagne visait à inciter les particuliers, les familles, les entreprises et les organisations des secteurs privés et public à reconnaître la nécessité d'être informés des risques et de leur sécurité sur Internet. On peut par ailleurs lire sur le site du ministère de sécurité publique au Québec<sup>44</sup> : « Le nombre estimé de vols d'identité était de 338 000 en 2006-2007 au Québec, pour un peu plus de 240 000 victimes ».

Il est intéressant de noter que les catégories de vol d'identité représentant le plus grand Pourcentage de victimisation sont respectivement l'utilisation de carte de débit ou crédit avec 3% et les informations personnelles compromises sans fraude avec 2,5 %. Ce qui met les sites de **E-commerce** en première ligne pour faire l'objet d'efforts de sécurisation. Mais comme on peut noter sur le nouveau blogue de Benoît Dupont<sup>45</sup>, « une question légitime serait celle de l'efficacité d'une telle campagne » et de souligner que « Il est certain par contre qu'une campagne de sensibilisation au vol d'identité ne devrait pas nécessairement se focaliser sur les seules transactions en ligne. En effet, dans une étude menée plus tôt cette année, nous avons montré que les voleurs d'identité n'utilisent Internet pour acquérir l'identité de leur victime que dans un peu moins de 20% des cas.»

Fin Octobre, on pouvait apprendre sur le Blog de Vincent Gautrais<sup>46</sup> la sanction royale du projet de loi S-4 modifiant le Code criminel (vol d'identité et infractions connexes). Ainsi, deux nouvelles infractions, assujetties à une peine maximale de cinq ans, sont créées dans la nouvelle section « Vol d'identité et fraude à l'identité » du Code criminel.

Cependant, l'éducation de l'internaute reste primordiale. En mai 2009, un hacker qui se fait appeler « Hacker Croll » avait réussi à pirater Twitter et publier des informations sensibles sur le Web les concernant. Pour dérober des données, le pirate s'était introduit sur un compte email Yahoo d'un employé de Twitter, en abusant déjà le système de récupération de mot de passe (en devinant la question secrète)<sup>47</sup>. Il a eu accès aux comptes Paypal, Amazon, Apple, AT&T, MobileMe et Gmail d'Evan Williams (PDG de Twitter) ainsi que d'autres employés de Twitter<sup>48</sup>. Histoire riche d'enseignements comme le précise le pirate sur Techcrunch « J'espère que mes interventions répétées auront permis de montrer à quel point il peut être facile à une personne mal intentionnée d'accéder à des informations sensibles sans trop de connaissances.»<sup>49</sup>, elle nous permet de tirer des leçons comme ne pas avoir le même mot de passe pour tous les comptes, se méfier des questions secrètes (verrou) et Changer le mot de passe mail régulièrement.

### VI.1.b Solutions proposées

On aura donc vu que le vol d'identité est un danger sérieux pour la société et une entrave majeure pour le développement de notre activité de commerce électronique tellement elle suscite les craintes et réticences des cybers acheteurs potentiels. Toutefois des solutions existent et d'autres sont proposées en laboratoire, nous allons faire un survol de celles-ci. Primo, il s'agit de s'assurer de la protection de la vie privée des individus en protégeant leurs informations personnelles entrées via les réseaux sociaux ou sites e-commerce.

La haute autorité en matière d'Internet « W3C » lançait en 2002 son projet P3P (Platform for Privacy Preferences Project<sup>50</sup>) qui en résumé est un ensemble standardisé de questions à choix multiples, couvrant ainsi les aspects essentiels de la vie privée d'un site Web donné. L'ensemble des réponses, présentées sous la forme d'un document XML, constitue la déclaration sur la vie privée, lisible par une machine. Il s'agit d'un cliché clair qui indique comment sont traitées les données personnelles des utilisateurs. Les navigateurs reconnaissant P3P peuvent 'lire' automatiquement cette déclaration et la comparer aux préférences personnelles de l'internaute. P3P améliore le contrôle de l'utilisateur en plaçant les déclarations de la vie privée là où il peut les trouver, en les formatant pour qu'il puisse les comprendre et plus important, en l'autorisant à agir selon le résultat de la comparaison entre déclaration du site Web et préférences de l'utilisateur.

Toutefois, cette technique n'impose aucunement aux sites de respecter les politiques ainsi affichées en plus d'entraver la navigation de l'internaute à l'image des 'alertes cookies'<sup>51</sup>. D'autres techniques ont été lancées en même temps appelée PETs (Privacy enhancement technologies) qui peuvent être définies ainsi : Protocoles, standards et outils qui participent directement à la protection de la vie privée en limitant la collecte des données à caractère personnel et, quand cela est possible, en supprimant cette collecte<sup>52</sup>. Ainsi, Zero-Knowledge avait développé un logiciel Web garantissant l'anonymat sur Internet. Des sociétés comme Privacyx.com et Anonymizer.com, proposent des serveurs leurres : quand vous voulez accéder à un site sécurisé, il ira d'abord se brancher sur un de ces serveurs d'anonymat avant de demander à ce dernier d'accéder au document désiré. Celui-ci va chercher le document et le renvoie sous sa propre adresse. Mais des serveurs officiels comme Anonymizer sont trop réputés et par conséquent sont faciles à bloquer. De plus, selon Eloise Gratton, ces logiciels de protection pourraient être contraires aux

lois concernant le cryptage en droit canadien, américain et français.»<sup>53</sup>. Cette initiative n'a donc pas connu le succès escompté et ces techniques ne se sont pas assez répandues. Par ailleurs, une autre technique (par opposition aux attaques non techniques telles que le « social engineering »), il y a aussi le phishing ou hameçonnage comme a été le cas des clients Ebay en 2003 ou récemment en Octobre 2009 où la direction générale des finances publiques a du intervenir pour mettre en garde les internautes des faux emails des Impôts qui circulaient sur la toile. L'Anti-Phishing Working Group (APWG) est l'association industrielle qui se consacre à la mise en application des lois axées sur l'élimination de la fraude et l'usurpation d'identité par phishing, le pharming et le courrier électronique de tous types. On peut lire sur leur site antiphishing.com que le mois de Juin dernier enregistrait le deuxième record des attaques depuis la mise en place de l'outil statistique avec plus de 49 000 sites de phishing uniques ! L'APWG propose son répertoire de solutions classées pour faciliter le choix du logiciel adéquat<sup>55</sup>. On compte également parmi les acteurs majeurs dans la supervision des cyber crimes en commerce électronique le Computer Security Institute (CSI), une organisation à but non lucratif qui travaille de concert avec le FBI de San Francisco pour mesurer les impacts et évolutions de ceux-ci. En 2004, ils avaient publié un rapport des tendances alarmant basé sur les analyses du Computer Emergency Response Team (CERT), qui relevait que les attaques étaient à la hausse, Trois équipes de l'université Carnegie Mellon y travaillent<sup>54</sup>. Les grandes questions de sécurité qui concernent la protection de la vie privée dans le cadre du commerce électronique, peuvent être résumées comme suit : authentification, autorisation, vérification des privilèges, confidentialité, intégrité et non répudiation. Le cryptage du contenu répond à ces questions en combinant plusieurs techniques telles que clés publiques, clés privées et clés symétriques avec la fonction de hashage, signature électronique et certificat électronique délivré par l'autorité compétente. (PKI plus SSL). Les systèmes biométriques proposent des solutions déjà sur le marché : reconnaissance faciale, empreinte digitale, contrôle de l'iris ou la voix...Etc. Une autre méthode en développement consiste à échantillonner la manière d'utiliser le clavier par l'utilisateur et ainsi établir une norme pour celui-ci. De même sur le site du consortium biométrique (biometric.org), on peut trouver la liste des vendeurs et toutes les technologies commerciales disponibles.

Pour une meilleure protection, il faut se doter d'**antivirus**, **anti spyware/adware**, **antimalware** et **pare feu** qui répondent aux normes de sécurité souhaitée tout en prenant soin de bien effectuer les réglages nécessaires en fonction du risque estimé.

D'autres mesures de protection peuvent être prises en fonction du degré d'exposition.

Par exemple, on peut utiliser une application qui va masquer l'adresse IP sur Internet.

**Privacy Pro** assure qu'avec ce système, le vol d'identité sur Internet ne sera plus possible parce que les voleurs ne seront pas en mesure d'obtenir vos informations privées<sup>55</sup>. Pour protéger les données, Il y a une panoplie de logiciels tels qu'**Internet Privacy**

**Protection Tool**. Il sert à nettoyer toutes les traces d'activité sur Internet et répond à la norme du gouvernement des USA en matière de protection des données personnelle<sup>56</sup>.

Sur le site d'EPIC, on trouve une liste d'outils pour la protection de vie privée.<sup>57</sup>

Pour rendre ses données et sessions internet confidentielles, la protection de la vie privée est à mettre dans un contexte particulier et donc les solutions logicielles sont différentes.

Par exemple, pour rendre ses données illisibles sur un PC portable, qui peut être volé, le cryptage s'impose. Il faut choisir un mot de passe long et bien sécurisé et conserver le fichier clé à l'abri. La solution de **Steganos** offre en plus la possibilité de cryptage de messagerie et données Outlook...Dans le domaine de la stéganographie (la dissimulation)

on peut opter pour **ArchiCrypt**. Par ailleurs, En surfant sur Internet, le système d'exploitation et les programmes utilisés stockent de nombreux fichiers qui peuvent compromettre la vie privée. Pour effacer donc ses traces sur Internet il y a **Anti Tracks**.

La cryptographie est justifiée par l'importance de sécuriser des données confidentielles, de préserver les secrets commerciaux et de protéger la vie privée. En plus de garantir la confidentialité des données, elle garantit aussi leur intégrité et leur authenticité : **PGP**.

Une autre mesure de protection de la vie privée : l'anonymat du surf, qui s'appuie sur des serveurs proxy anonymes, solution assez efficace mais ralentie la navigation : **JAP**.

Enfin, il ne faut pas oublier que malgré toutes ces techniques, on n'est pas à l'abri d'une intrusion, d'où l'intérêt d'un logiciel genre **SEAGATE**. Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer les activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

## VI.2 Vente de profils de consommation

La question d'établissement du profil des utilisateurs d'Internet afin d'accroître la valeur de la publicité pour l'annonceur, les éditeurs et les consommateurs, a été discutée lors de la table ronde sur les questions soulevées par l'ère numérique à Londres en Juin 2008. La commissaire européenne chargée de la protection des consommateurs, a précisé : « Le commerce électronique favorise la spécialisation et l'existence de marchés de niche. Cela est partiellement dû au fait qu'il permet aux publicitaires de cibler de manière efficace les marchés de niche. Les données sur les utilisateurs pouvant être recueillies via Internet rendent ce ciblage de plus en plus facile et efficace<sup>58</sup> ». En effet, il existe un marché parallèle de vente de ces profils, non contrôlé ni par les autorités ni par les utilisateurs. Ici au Canada, un an plus tôt, on apprenait selon l'allocution prononcée à l'occasion de la conférence '*Internet Law - The Second Wave: New Developments, Challenges and Strategies*' : « Il existe maintenant en ligne toute une industrie de courtage de données qui se spécialise dans la compilation, l'analyse et la vente de renseignements personnels à des personnes et à des organisations. D'après l'Association canadienne du marketing, le secteur du marketing au Canada génère plus de 480 000 emplois et entraîne, par l'intermédiaire de différents réseaux commerciaux, des ventes annuelles totales de plus de 51 milliards de dollars. Une grande partie de cette activité économique se traduit par l'analyse, l'utilisation et le partage de renseignements sur les consommateurs<sup>59</sup> ». Il s'agit donc d'un véritable fléau où seule l'implication de l'utilisateur peut le réduire.

## VI.3 Constitution de dossiers sur les personnes

Nous avons évoqué le fantasme de « Big Brother », au sujet de la possibilité pour autrui ou pour un pouvoir institué, de tout connaître d'un individu, lors de l'avènement de l'ère informatique. Aujourd'hui, grâce au recoupement de plusieurs informations disponibles en lignes sur les réseaux sociaux, les forums, blogs et autres, cela est rendu possible. Octobre 2009, Mediapost annonçait que les agences de renseignements américaines allaient disposer d'un outil pour lire les billets de blogs, les tweets et les discussions sur Internet, en profitant de l'injection de nouveaux capitaux du In-Q-Tel, fonds américain de capital-investissement à but non lucratif créé et géré par la Central Intelligence Agency<sup>60</sup>. De l'autre côté de l'atlantique, le 25 Novembre 2009, on pouvait lire dans l'Express belge que La police américaine utilise Facebook pour surveiller les jeunes américains<sup>61</sup>.

Il apparaît donc évident qu'il ne peut y avoir une vie privée sur Internet, quand bien même c'est l'état qui traite les informations. La collecte de renseignements sur une personne sans son consentement est une atteinte à la vie privée, protégée par la déclaration universelle des droits de l'Homme et par Code civil. En plus le projet de suivre en permanence les activités de chacun n'est pas compatible avec une société de libertés. Cela nous amène encore une fois à sensibiliser l'utilisateur quant à l'utilisation d'internet qui est un lieu de partage mais aussi de divulgation de renseignements divers.

#### **VI.4 Monitoring des salariés**

L'effet des réseaux sociaux touche désormais également le milieu professionnel. Le temps passé d'un employé à partager sur un réseau social avec ses relations, est autant de temps perdu par l'entreprise. Le magazine Forbes publiait en Octobre 2009 que des sites comme Facebook et Twitter coûtait à l'économie anglaise 2,3 milliards de dollar comme temps perdu selon une étude de TSN<sup>62</sup>. Aux États-Unis, une étude de Robert Half Technology<sup>63</sup>, cabinet de recrutement, révélait que 54% des entreprises des États-Unis disent interdire les travailleurs d'utiliser les sites de réseautage social comme Twitter, Facebook, LinkedIn et MySpace, au travail. Les réseaux sociaux créent une certaine dépendance et les employés peuvent y diffuser du contenu concernant leurs employeurs. Ici au Canada, et selon une étude menée par Harris Interactive, pour le compte de CareerBuilder<sup>64</sup>, en juin 2009, il apparaît que ces sites pèsent donc de plus en plus dans la décision de recrutement. 26 % des employeurs canadiens utilisant les réseaux sociaux déclarent que l'information qu'ils y ont trouvée les a déjà dissuadés de recruter un candidat : photo inappropriée pour 55 % d'entre eux, partage d'informations confidentielles sur un précédent employeur (50 %), commentaire discriminatoire (38 %), évocation d'alcool ou de drogue (36 %), mensonge sur les qualifications (26 %),...

Ainsi donc certains aspects de la vie privée étalée au grand jour sur Facebook peuvent intéresser l'employeur. Le cas récent de Nathalie Blanchard qui s'est vue suspendre les indemnités de congé maladie à cause de photos publiées sur Facebook et dénoncées par son employeur, a fait le tour du monde. Il en ressort que les entreprises vont avoir recours dans l'avenir à des techniques de monitoring on line. Mais, cette nouvelle manière d'espionner pose des problèmes d'éthique comme le soulignait le travail du département management et technologie de l'UQAM : « La surveillance des employés branchés<sup>65</sup> ».

### **VI.5 E-réputation de l'entreprise**

Selon un site dédié à cette notion, nous pouvons noter qu'elle se définit sous forme d'un nuage de tags, représentatif de ce qui se dit de l'entreprise sur Internet et le concept : « L'e-réputation est l'image que les internautes se font d'une marque ou d'une personne. Cette notoriété numérique façonne l'identité d'une marque, la différenciant de ses concurrentes<sup>66</sup> ». Notons qu'un site existe pour la mesure de celle-ci : [howsociable.com](http://howsociable.com). Cette nouvelle notion est le résultat du succès des réseaux sociaux et l'importance de leur influence dans la réputation d'une marque ou entreprise. Pour en mesurer l'envergure, il suffit de prendre connaissance du projet Google Social Search<sup>67</sup>, qui prévoit d'intégrer dans les résultats de recherche les avis et commentaires émis par les membres faisant partie de notre réseau social au sens large. Nous comprenons donc l'intérêt pour l'entreprise et ses salariés de suivre ce qui se dit sur ces réseaux la concernant. Il s'agit d'un jeu à hauts risques auquel devront se livrer les marques et entreprises, car il a des effets positifs comme nous allons le voir, mais le côté sombre est l'absence de contrôle de ces informations comme dans le cas de la vie privée de la personne.

## **VII. Usage des médias sociaux pour l'entreprise**

### **VII.1 Marketing viral**

Comme nous avons vu, les réseaux sociaux se sont développés avec le WEB 2.0 avec sa culture partagée par la communauté des internautes et son intelligence collective. Les spécialistes s'accordent à lui reconnaître la double dimension sociale et technologique. En marketing, le bouche à oreille (Word of Mouth) occupe une place de choix dans la stratégie de communication. Les consommateurs lui accordent une crédibilité supérieure à la communication formelle et non objective émanant de l'entreprise. Le Web 2.0 fournit tous les moyens de développer le bouche à oreille (BAO) grâce aux possibilités données aux consommateurs d'exprimer leur expérience au sein des blogs, des forums, des chats et des réseaux sociaux en plus d'évaluer les cybers marchands sur les sites comparatifs. Contrairement au BAO, le marketing viral n'est pas spontané. Des outils sont mis en place pour favoriser et amplifier une communication positive autour d'un produit ou d'une marque. Les consommateurs communiquent un message à d'autres consommateurs via internet en échange de bonis de l'entreprise. Facebook compte plus de 45 millions de pages de Groupes. Les listes de Twitter peuvent être également fort utiles dans ce cas

## VII.2 Lancement de produits et branding

Le buzz marketing n'est qu'une technique parmi d'autres du marketing viral qui vise à créer une rumeur ou un brouhaha médiatique avant la sortie d'un produit. Si Google est un excellent produit de marketing viral avec ses communautés de webmasters, universitaires, journalistes, documentalistes et tous les professionnels de la recherche de l'information, la S40 de Volvo est un très bon exemple de buzz marketing. Volvo avait alors choisi pour le lancement de la S40 d'initier une rumeur autour du « mystère de Dalarô », des messages alors avaient été postés sous de fausses identités dans les forums et des identités fictives ont été créées pour propager la rumeur dans les réseaux sociaux. Dans la dernière édition '*le e-marketing à l'heure du web 2.0*'<sup>68</sup> de C.Viot, elle introduit la notion d'objet sur lequel porte la communauté : une marque, un produit, une idée, un hobby, etc. La marque '*Harley Davidson*' est à l'origine d'un fan club. Il est plus facile de développer une communauté s'il existe un noyau de consommateurs déjà engagés à l'égard de la marque. Être membre de la communauté influence la fidélité à la marque. Les réseaux sociaux sont des ponts de lancement incontournables pour les campagnes de marketing viral comme vu précédemment, mais aussi peuvent servir une publicité sociale selon les termes de C.Viot. Il n'est donc pas étonnant que les marques convoitent leur audience pour assoir le « pouvoir de la marque » ou branding. Ford l'utilise très bien pour le rétablissement de sa marque légendaire.

## VII.3 Développement d'e-commerces

Les médias sociaux évoluent vers un lieu où les consommateurs vont nicher en ligne. Ils ne sont plus là seulement pour avoir des conversations. Ils partagent des photos. Ils jouent des jeux. Ils cherchent des informations. Ils utilisent les réseaux sociaux pour les aider à prendre des décisions d'achat. Parfois, cela passe par la conversation. Parfois, c'est le fait d'être un fan de la page Facebook d'une marque et de recevoir des mises à jour en temps opportun. Facebook dispose d'une monnaie virtuelle, et commence à ouvrir des possibilités d'achats de biens physiques. Facebook Connect a été optimisé pour que les webmasters déploient ces moyens sur leurs sites. Les gens passent beaucoup de temps sur Facebook, ils placent une grande confiance dans le réseau social. Si le site d'e-commerce est couplé au réseau et que le consommateur peut s'y connecter, alors il sera plus à l'aise pour effectuer ses achats. Une histoire simple démontre leur influence en e-commerce<sup>69</sup>.

## VIII. Conclusion

En conclusion de cette étude, nous pouvons retenir trois points principaux :

- ✚ Le challenge actuel du web 2.0 est de dépasser les craintes des usagers concernant la protection de leur vie privée
- ✚ Les réseaux sociaux sont à l'origine de menaces de détournement d'information et aussi des failles en sécurité informatique.
- ✚ L'industrie du commerce en ligne doit intégrer ces média dans leur stratégie de marketing web et profiter de cette confiance dont ils jouissent.

Concernant la protection de la vie privée, il faut multiplier davantage les campagnes de sensibilisation des consommateurs pour qu'ils soient plus vigilants concernant la divulgation de leurs informations. Toute demande de renseignement supplémentaire non nécessaire à la réalisation de la transaction devrait être simplement refusée comme le stipule la loi de protection des renseignements personnels au Canada. En même temps, ils devraient bénéficier de conseils quant à l'utilisation des différentes solutions (offres logicielles) commerciales existantes pour rendre la tâche des fraudeurs plus ardue. Bien que les lois qui régissent les vols d'identité existent, elles sont peu efficaces. Il faudrait les appliquer de manière dissuasive et les renforcer au vu des nouveaux cas. Dans la relation entreprise salarié, de nouvelles règles doivent être mises en place de manière formelle qui fixent les conditions de comportement de ces derniers sur les médias sociaux quand il s'agit de parler de leur entreprise. Celle-ci pour sa part doit encourager ses employés à promouvoir et défendre ses intérêts sur Internet.

Dans la stratégie internet qui se borne à avoir un site web qui constitue la vitrine de l'entreprise, il faudra inclure une démarche spécifique pour construire et défendre l'e-réputation via les outils du web 2.0 (blogs, forum, réseaux sociaux, sites comparatifs.etc). Les sites d'E-commerce devraient se rapprocher des réseaux sociaux et construire des passerelles avec ceux-ci pour capter le consommateur dans un environnement sécurisant.

De la même manière que la FTC étudie le moyen de responsabiliser les bloggeurs en les obligeant à déclarer leurs revenus, il faudrait transposer cet outil aux réseaux sociaux.

## Bibliographie

Liste des ouvrages et URLS par ordre alphabétique (dernier accès 30 Novembre 2009)

- 1 Glenn CHAPMAN 1 :  
[http://www.google.com/hostednews/afp/article/ALeqM5hDhd0kwSVQa\\_qQ9hZEvI\\_EgqdDumg](http://www.google.com/hostednews/afp/article/ALeqM5hDhd0kwSVQa_qQ9hZEvI_EgqdDumg)
- 2 Safe Harbour Privacy Principles 2 : <http://www.e-juristes.org/content/les-%C2%AB%C2%A0safe-harbor-privacy-principles%C2%A0%C2%BB>
- 3 Définition de réseau social 3 :  
[http://www.journaldunet.com/encyclopedie/definition/1053/41/21/social\\_networking.shtml](http://www.journaldunet.com/encyclopedie/definition/1053/41/21/social_networking.shtml)
- 4 Vote de la loi 410-15 aux USA 4 :  
<http://pascalbeauchesne.wordpress.com/2007/09/05/historique-des-reseaux-sociaux-de-aol-a-facebook/>
- 5 Domination de Facebook 5 :  
[http://www.ofcom.org.uk/advice/media\\_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf)
- 6 Twitter 6 : <http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/>
- 7 Barack Obama, candidat des réseaux 7 : <http://blog.mondediplo.net/2008-04-21-Barack-Obama-candidat-des-reseaux-sociaux-sur>
- 8 A Comparative Analysis of Six Sites 8 : Barrigar, J., (2009) "Social Network Site Privacy: A Comparative Analysis of Six Sites", The Office of the Privacy Commissioner of Canada.
- 9 Fred Cavazza 9 : <http://www.fredcavazza.net/2008/05/19/panorama-des-medias-sociaux/>
- 10 Personnaliser les pages de profil 10 :  
[http://music.lovetoknow.com/History\\_of\\_Myspace](http://music.lovetoknow.com/History_of_Myspace)
- 11 Keep it Simple, Stupid 11 : <http://www.techcrunch.com/2009/04/28/keep-it-simple-stupid/>
- 12 Evan Williams 12 : <http://fr.wikipedia.org/wiki/Twitter>
- 13 Nielsen Twitter 13 : <http://blog.nielsen.com/nielsenwire/nielsen-news/twitter-grows-1444-over-last-year-time-on-site-up-175>
- 14 LinkedIn 14 :  
[http://www.linkedin.com/static?key=user\\_agreement&trk=hb\\_ft\\_userag](http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag)
- 15 R.Gervais, PDG de Zerofail 15 :  
<http://lapresseaffaires.cyberpresse.ca/economie/200901/06/01-688930-linkedin-un-reseau-social-pour-les-affaires.php>
- 16 LinkedIn 40 millions de membres 16 : <http://press.linkedin.com/history>
- 17 Viadeo en novembre 2006 17 : <http://corporate.viadeo.com/fr.html>
- 18 LinkedIn & Twitter 18 : <http://blog.linkedin.com/2009/11/09/allen-blue-twitter-and->

- linkedin-go-together-like-peanut-butter-and-chocolate/
- 19 Politiques en matière de vie privée Facebook 19 :  
<http://www.facebook.com/policy.php?ref=pf>
  - 20 Affaire Beacon 20 : <http://www.generation-nt.com/facebook-publicite-zuckerberg-beacon-actualite-50396.html>
  - 21 Suppression des données Facebook 21 :  
<http://www.nytimes.com/2008/02/11/technology/11facebook.html>
  - 22 Nouvelle version de politique de confidentialité Facebook 22 :  
<http://www.gautrais.com/Facebook-propose-sa-nouvelle>
  - 23 Politique de Confidentialité de Myspace 23 :  
<http://www.myspace.com/index.cfm?fuseaction=misc.privacy>
  - 24 Politique de Confidentialité de Twitter 24 : <http://twitter.com/privacy>
  - 25 Politique de Confidentialité de LinkedIn 25 :  
[http://www.linkedin.com/static?key=privacy\\_policy&trk=hb\\_ft\\_priv](http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv)
  - 26 Politique de Confidentialité de Viadeo 26 : <http://www.viadeo.com/aide/cgv/>
  - 27 Myspace music 27 : <http://www.zdnet.fr/blogs/digital-jukebox/tous-les-dessous-du-lancement-de-myspace-music-39601927.htm>
  - 28 Fonctionnalités payantes pour les comptes commerciaux Twitter 28 :  
<http://archives.chicagotribune.com/2009/oct/07/business/chi-biz-twitter-graphic-oct07>
  - 29 Pôle Job/Publicité/Formation Viadeo 29 :  
<http://lastexittomymind.wordpress.com/2009/08/19/le-business-model-des-reseaux-sociaux-professionnels/>
  - 30 Mise en commun d'informations WEB 2.0 30 : [http://fr.wikipedia.org/wiki/Web\\_2](http://fr.wikipedia.org/wiki/Web_2)
  - 31 Mobilisation effective des compétences web 2.0 31 :  
<http://www.internetactu.net/2004/02/11/quest-ce-que-lintelligence-collective/#note>
  - 32 ReST 32 : <http://www.xfront.com/REST-Web-Services.html>
  - 33 Wikis 33 : <http://fr.wikipedia.org/wiki/Wikis>
  - 34 ASP 34 : <http://fr.wikipedia.org/wiki/SaaS>
  - 35 Tendances réseaux sociaux 2010 35 :  
[http://blogs.harvardbusiness.org/cs/2009/11/six\\_social\\_media\\_trends.html](http://blogs.harvardbusiness.org/cs/2009/11/six_social_media_trends.html)
  - 36 Google Wave 36 : <http://www.web-libre.org/breves/google-wave,10147.html>
  - 37 Google Latitude 37 : <http://www.marketing-internet-montreal.com/2009/11/reseaux-sociaux-localisation/>
  - 38 210.000 victimes, Figaro 38 : <http://www.csoonline.com/article/print/496314>
  - 39 LOPPSI 39 : <http://www.loppsi.fr/app/4,loppsi.pdf>
  - 40 CSO 40 : <http://www.lefigaro.fr/actualite-france/2009/10/06/01016-20091006ARTFIG00305-usurpation-d-identite-plus-de-210000-victimes-par-an.php>
  - 41 Le vol d'identité 41 :

- [http://isiq.ca/particulier/campagne\\_sensibilisation/protection\\_identite/comprenez\\_vol\\_identite/index.html](http://isiq.ca/particulier/campagne_sensibilisation/protection_identite/comprenez_vol_identite/index.html)
- 42 Guy Laliberté victime d'usurpation 42 :  
<http://fr.canoe.ca/divertissement/livres/nouvelles/2009/09/10/10819306-jdm.html>
- 43 FBI 43 : <http://www.fbi.gov/pressrel/speeches/mueller100709.htm>
- 44 Ministère de sécurité publique au Québec 44 :  
[http://www.msp.gouv.qc.ca/prevention/prevention.asp?txtSection=statistiques&txtCategorie=vol\\_identite](http://www.msp.gouv.qc.ca/prevention/prevention.asp?txtSection=statistiques&txtCategorie=vol_identite)
- 45 Benoît Dupont 45 : <http://crimes-cyber.blogspot.com>
- 46 Blog de Vincent Gautrais 46 : <http://www.gautrais.com/Vol-d-identite-le-projet-de-loi>
- 47 Hacker Croll 47 :  
<http://www.zdnet.fr/actualites/internet/0,39020774,39702110,00.htm>
- 48 Vol d'identités employées de Twitter 48 : <http://www.korben.info/hack-de-twitter-la-suite.html>
- 49 Techcrunch 49 : <http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>
- 50 P3P 50 : <http://www.w3.org/P3P/>
- 51 Alertes cookies 51 : <http://www.symantec.com/region/fr/resources/protocole.html>
- 52 PETs 52 : <http://www.w3.org/2002/p3p-ws/pp/epic.pdf>
- 53 Eloise Gratton 53 : <http://www2.lex-electronica.org/articles/v7-2/gratton.htm>
- 54 Carnegie Mellon 54 : Turban, E., King, D., Viehland, D., Lee, J. (2006) Electronic Commerce, a Managerial Perspective, Prentice hall, pp 459-460
- 55 APWG 55 : <http://www.privacy-pro.com/identity-theft-protection.html>
- 56 Protection Tool 56 : <http://www.cs.virginia.edu/felt/privacybyproxy.pdf>
- 57 Liste d'outils EPIC 57 : <http://internet-privacy-protection.smartcode.com>
- 58 Publicités ciblées 58 : Principaux enjeux de la politique des consommateurs à l'ère numérique
- 59 Vente de renseignements personnels Canada 59 :  
[http://www.priv.gc.ca/speech/2008/sp-d\\_080327\\_lc\\_f.cfm](http://www.priv.gc.ca/speech/2008/sp-d_080327_lc_f.cfm)
- 60 In-Q-Tel 60 :  
[http://www.mediapost.com/publications/?fa=Articles.showArticle&art\\_aid=115661](http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=115661)
- 61 Express belge 61 : <http://www.express.be/business/fr/technology/la-police-amricaine-utilise-facebook/117101.htm>
- 62 TSN 62 : <http://www.forbes.com/2009/10/26/twitter-facebook-costs-markets-faces-guidelines.html>
- 63 Robert Half Technology 63 :  
<http://www.zdnet.fr/actualites/internet/0,39020774,39708929,00.htm>
- 64 CareerBuilder 64 : <http://www.humanresourcesjobs.ca/newsletter/employeurs-canadiens-utilisent-reseaux-sociaux-ligne-l-fr-i-805.html>

- 65 La surveillance des employés branchés 65 :  
<http://www.fsa.ulaval.ca/personnel/vernag/EH/F/manif/lectures/surveillance%20des%20employ%C3%A9s.pdf>
- 66 E-réputation de l'entreprise 66 : <http://www.e-reputation.org/definition-e-reputation-105>
- 67 Google Social Search 67 : [http://www.youtube.com/watch?v=ZqWJxgp-\\_mU&feature=player\\_embedded](http://www.youtube.com/watch?v=ZqWJxgp-_mU&feature=player_embedded)
- 68 Viot, C 68 : Le e-marketing à l'heure du Web 2.0. (2009) Gualino editeur
- 69 Vidéo Youtube influence des réseaux en e-commerce 69 :  
[http://www.youtube.com/watch?v=MpIOCIX1jPE&feature=player\\_embedded](http://www.youtube.com/watch?v=MpIOCIX1jPE&feature=player_embedded)

Mohammed ALAMI