Guy-Hermann Ngambeket Ndiandukue, CISA, CISM, CGEIT, ITIL V3(F), PMP, est Ingénieur en informatique et exerce en tant que consultant à PwC Cameroun. Il a effectué des missions d'audit pour le compte de multiples entreprises appartenant à des secteurs aussi variés que la banque, les télécommunications, l'assurance et l'industrie métallurgique, entre autres. Il également spécialise en analyse de données. Il peut être contacté à *guy.hnd@gmail.com.*

Réseaux Sociaux et Vie Privée: Menaces et Protections

«Broadcast yourself!» littéralement «Diffusez vous-mêmes!», le slogan de YouTube pourrait à lui seul résumer l'esprit de la révolution sociale provoquée par la déferlante des réseaux sociaux. Ces derniers s'imposent désormais comme l'un des principaux canaux de communication sur la toile: des liens de toutes natures s'y créent, s'y développent et s'y rompent de façon quasi-instantanée.

Selon une étude[1] publiée en France par l'IFOP (Institut Français d'Opinion Publique) sur les réseaux sociaux, menée auprès d'un échantillon de 1,002 personnes âgées de 18 ans et plus, 77 pourcent des Internautes déclarent être membre d'au moins un des réseaux sociaux en ligne testés dans l'étude.

De fait, la notoriété de ces réseaux sociaux derniers ne résulte pas d'un simple effet de mode. Ils permettent à leurs membres de joindre utile et agréable en offrant une panoplie d'applications et d'avantages adaptés à leur public cible. Par exemple, LinkedIn constitue un marché géant de l'emploi, par exemple: Jeff Epstein, responsable financier d'Oracle, aurait été recruté grâce à son profil sur ce réseau.[2]

Cependant, il serait illusoire de penser que cette croissance exponentielle des réseaux sociaux comporte seulement des effets positifs. En effet, la publication et le partage d'informations très personnelles, exposent les Internautes à tous types d'abus et de violation de leur vie privée. Ainsi, en 2009, une jeune femme a-t-elle été licenciée pour avoir utilisé Facebook durant son arrêt de travail dû à des migraines lors de l'utilisation des ordinateurs. Son patron a déclaré que si elle pouvait utiliser Facebook, elle était en mesure de travailler sur ordinateur. Cet incident a lancé la question de l'espionnage via Facebook.[3]

Cet article a un double objectif: partir des motivations des Internautes à fréquenter les réseaux sociaux en vue d'identifier le risque de violation de leur vie privée, et d'analyser et évaluer l'efficacité des moyens de contrôle de lutte mis en œuvre.

MOTIVATION DES INTERNAUTES

Une étude publiée par le cabinet Deloitte[4] en avril 2011 affirme que la «connexion permanente au maximum d'amis est la fonction principale pour la majorité des populations» connectées aux réseaux sociaux. Ce constat ne signifie pas pour autant que cette fonction fasse l'unanimité parmi la totalité des utilisateurs des sites. En effet, les membres de réseaux sociaux sont loin de former une population homogène. Selon l'âge et le milieu socioprofessionnel, on trouve plusieurs catégories ayant chacune des centres d'intérêt différents. **Illustration 1** suivant présente de façon succincte les principaux groupes d'utilisateurs et leurs motivations à utiliser les réseaux sociaux.

Illustration 1—Catégories D'utilisateurs de Réseaux Sociaux

Groupe	Motivations
Particuliers	Interaction avec les proches, recherche et opportunités professionnelles
Employeurs, recruteurs	Profilage psychologique et social des postulants
Criminels	Spams, arnaques et crimes sexuels
Police, armée, services secrets et agences gouvernementales	Profilage du personnel, enquêtes criminelles, communication rapide avec la population notamment par le biais de Twitter
Politiciens et activistes	Propagande idéologique, recherche et jauge de popularité
Entreprises	Profilage et ciblage des marchés potentiels, approfondissement de la relation client, promotion et vente en ligne, sondages et études en ligne

Figure 1 montre que le groupe le plus vulnérable est celui des particuliers qui constituent la majorité des utilisateurs des réseaux sociaux. En effet, les autres catégories se

servent librement des informations publiées par ces derniers à des fins diverses.

Quel est donc le risque encourus par les centaines de millions de personnes connectées à Facebook, LinkedIn, Twitter, ou Myspace?

RISQUE

Chaque Internaute connecté aux réseaux sociaux possède une identité numérique. Elle se forge à partir de tout ce qu'il publie sur ses différents comptes et permet de dresser une sorte de "portrait robot" de sa personnalité. "A chaque connexion, envoi de courriel, lancement d'une recherche sur un moteur, ce sont des contenus de conversations privées, des adresses IP, des adresses de sites visités qui sont archivés, et éventuellement exploités à des fins commerciales [...]".[5]

Les enjeux financiers ou stratégiques de l'accès à cette identité par divers groupes d'intérêts sont dès lors évidents. De ce fait, à risque menace les utilisateurs de réseaux sociaux et la sécurité des données partagées sur les réseaux sociaux:

- **Usurpation d'identité**—L'accès aux informations de base constituant l'identité de l'internaute (par exemple, nom, prénom, date de naissance, lieu de naissance, photo) ouvre la voie au risque d'usurpation d'identité. En France, ce risque a été reconnu et a mené à faire évoluer la législation. Ainsi, un nouvel article 226-4-1 de la loi dite Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI 2) a été adoptée par le législateur français le 8 février 2011.[6]
- **Pédophilie et crimes sexuels**—Les adolescents, plus nombreux et plus actifs sur les réseaux sociaux, y sont exposés à des prédateurs sexuels. Ces derniers ont en effet le loisir d'entrer en contact avec leurs victimes, la plupart du temps sous une fausse identité, et de les localiser géographiquement. Ce risque est d'autant plus grand que les adolescents sont moins enclins que les adultes à être prudents sur ces réseaux. Ainsi, un sondage effectué en 2006 aux États-Unis, dans le cadre d'une recherche menée par l'université de Princeton sur 935 adolescents révèle que:[7]
  - 4 adolescents sur 5 inscrivent leur prénom dans leur profil
  - 4 adolescents sur 5 postent leur photo, et 2 adolescents sur 3 celle de leurs amis. Quand on leur rappelle le caractère public de la publication de photos, la plupart d'entre eux ne se disent pas inquiets de risque pour leur vie privée. Ils pensent que les photos, même combinées avec les autres informations du profil, ne donnent pas assez de détails pour compromettre leur sécurité.
  - 6 adolescents sur 10 inscrivent le nom de la ville où ils habitent
  - 1 adolescent sur 2 inscrit le nom de son école
  - 4 adolescents sur 10 inscrivent leur pseudo de messagerie (par exemple, adresse MSN)
  - 3 adolescents sur 10 inscrivent leur nom de famille
  - 1 adolescent sur 10 inscrit son nom et prénom dans son profil public
  - 1 adolescent sur 20 inscrit son nom complet, sa photo, le nom de son école et le nom de sa ville dans son profil public
  - 2 adolescents sur 3 restreignent l'accès à leur profil (par exemple, en le rendant privé, en le protégeant par un mot de passe, en le cachant complètement à la vue des autres, etc.)

  Les résultats de cette enquête montrent bien la vulnérabilité des plus jeunes, et leur manque évident d'informations sur le risque d'attaques pédophiles à travers les réseaux sociaux. Il est à noter également le risque pour les adolescents de développer des traumatismes ou des dépendances face à certains contenus pornographiques et obscènes publiés sur ces sites.
- **Licenciement/disqualification/faute grave**—Certains réseaux sociaux comme Viadeo ou LinkedIn permettent à leurs utilisateurs de poster leur curriculum vitae (CV) et éventuellement de trouver des opportunités de carrière. Par contre, les publications d'une personne sur un réseau social généraliste comme Twitter ou Facebook peuvent porter un coup à ses ambitions professionnelles. En effet, un employeur peut tout à fait estimer que des photos obscènes ou des propos orduriers peuvent nuire à l'image de l'entreprise, et licencier l'employé fautif. Aux États-Unis 45 pourcent des employeurs fouillent les réseaux sociaux quand ils veulent recruter.[8]

Le débat sur l'intervention des entreprises dans le contrôle des contenus publiés par leurs employés actuels (ou potentiels) est assez complexe, le risque pour les entreprises étant réels. Par exemple, des pirates informatiques pourraient utiliser des informations laissées sur un réseau social par les employés d'une entreprise donnée pour tenter d'accéder au système d'information de cette dernière : les

informations telles que la date de naissance ou les noms et prénoms d'enfants peuvent en effet leur permettre de trouver des mots de passe. Pire encore, un administrateur système maladroit pourrait, par exemple en demandant de l'aide à ses pairs sur un site Internet, poster des informations sur la configuration de son système d'exploitation, ce qui serait, le cas échéant, tout bénéfice pour les hackers. Ainsi, un arbitrage doit-il être impérativement être fait par l'employé entre son comportement et les intérêts de l'entreprise qui l'emploie.

- **Harcèlement publicitaire/spam**—En 2011 Facebook a réalisé un chiffre d'affaires publicitaire de 4 milliards de dollars, selon sa directrice générale, Sheryl Sandberg.[9] Certes, les firmes font de l'affichage publicitaire sur le site, mais elles utilisent aussi et surtout les informations privées qui y sont publiées, en vue de mieux cibler leur communication. C'est également le cas de Twitter qui à travers à sa notion de "tweet sponsorisé", fournit aux annonceurs des statistiques détaillées sur le profil des utilisateurs. Ce système leur permet d'en savoir davantage sur les clients potentiels d'obtenir des sources de revenus substantiels. Les spams constituent une nuisance réelle, et le pire, c'est que les éditeurs de ces sites en sont tout autant victimes que les populations. Par exemple, à la mi-novembre 2011, Facebook a été victime d'une campagne de spams pornographiques apparaissant sur les fils d'actualité des utilisateurs.[10]

Il existe encore d'autres dangers liés à la protection de la vie privée sur les réseaux: hameçonnage (phishing) facilité grâce aux données laissées sur les réseaux sociaux, espionnage par les services gouvernementaux, manipulations idéologiques (ex: terrorisme, racisme). Ce risque c'exacerbés par le modèle économique des réseaux sociaux qui constitue une entrave à la mise sur pied d'une politique sérieuse de sécurité des données privées.

MODELE ECONOMIQUE ET POLITIQUE DE CONFIDENTIALITE

Modèle Economique

Le modèle économique des réseaux sociaux est essentiellement basé sur la constitution de bases de données énormes sur les Internautes pour lesquelles les entreprises et agences gouvernementales sont prêtes à débourser énormément d'argent. Dans ce contexte, il va sans dire que le respect de la vie privée n'est pas la première préoccupation des éditeurs de ces sites.

Ceux-ci créent toujours davantage d'applications potentiellement dangereuses pour la protection de la vie privée, et parfois installées par défaut sur chaque profil ainsi en est-il de "Places"[11], un système de géolocalisation, ou encore de "Timeline"[12], une sorte de biographie de l'utilisateur générée avec l'ensemble de ses publications sur son profil Facebook. Ces constats nous poussent à regarder de près les conditions d'utilisation et de confidentialité des réseaux sociaux.

Conditions D'utilisation et de Confidentialité des Réseaux Sociaux

"L'ère de la vie privée est révolue". Cette déclaration n'est pas celle d'un hacker à l'affût de comptes à pirater mais bien de Mark Zuckeberg, fondateur et président directeur général (PDG) de Facebook. Et si elle a provoqué un tollé général, elle a pourtant le mérite de refléter le peu d'importance que les réseaux sociaux accordent à la vie privée des utilisateurs.

Ainsi, si les conditions d'utilisation de Facebook affirment mettre un point d'honneur à respecter et à protéger les données des membres du site, une clause stipule plus loin: "Nous faisons tout notre possible pour faire de Facebook un service sûr, mais ne pouvons pas garantir la sécurité absolue. Pour ce faire, nous avons besoin de votre aide, ce qui inclut les obligations suivantes…" S'ensuit alors une série de recommandations.

En synthèse, les conditions d'utilisation des réseaux sociaux ne sont nullement de nature à garantir la sécurité aux Internautes et sont à dessein rédigées de manière à les décourager de les parcourir réellement. Les sites n'ont en effet aucun intérêt à ce que les utilisateurs découvrent certaines clauses leurs donnant les pleins pouvoirs sur la totalité des informations publiées. Ainsi, en 2009, Facebook s'arrogeait droit de propriété à vie sur toutes les données des utilisateurs même après leur désinscription du site. Le site s'est ensuite vu forcé de renoncer à cette clause discrètement introduite, face à la véritable levée de boucliers suscitée par cette décision.

En raison du comportement ambigu des éditeurs des sites, chaque consommateur doit, d'une part, être informé sur la législation en vigueur et, d'autre part, adopter une attitude responsable pour se protéger.

LEGISLATION

En février 2009, Alex Türk, président de la Commission Nationale de l'Informatique et des Libertés (CNIL), pointait du doigt un problème crucial "Les sociétés de droit américain

qui dominent l'Internet ne se sentent pas tenues par les règlementations européennes…"[13] En effet, il est quasiment impossible à l'heure actuelle de mettre sur pied une législation globale et contraignante sur la régulation des réseaux sociaux. La majorité des serveurs de ces réseaux étant situés aux États Unis la loi américaine s'applique et, malheureusement, elle reste relativement lacunaire à propos de la sécurité des données privées des Internautes.

A défaut d'avoir un moyen plus efficace de pression sur les administrateurs des réseaux, la Commission Européenne adopte pour l'instant deux stratégies:[14]

- La sensibilisation, par le biais de campagnes publicitaires destinées surtout aux mineurs
- L'autorégulation, qui table sur une action volontaire des réseaux sociaux

Cependant, force est de constater au regard des faits évoqués plus haut que lesdits réseaux sont peu enclins à assumer cette responsabilité sociale pour des questions évidentes d'intérêts pécuniaires et stratégiques. En témoigne le récent blâme aux États Unis de la Federal Trade Commission (FTC) à l'encontre de Facebook,[15] concernant la violation du droit à la vie privée des utilisateurs. Les reproches de la Commission sont: "Le réseau social Facebook a accepté les reproches de la FTC en ce sens qu'il a déçu les utilisateurs en leur disant qu'ils pouvaient eux-mêmes protéger la confidentialité de leurs informations personnelles, puis d'un autre côté, et ce, régulièrement, il partageait ces mêmes informations et les rendait publiques". Certes, Mark Zuckerberg affirme travailler à ce que ces "erreurs" ne se reproduisent pas. Cependant, il est évident pour le moment que les utilisateurs sont extrêmement vulnérables à toutes sortes d'abus et de violation de leur droit fondamental au respect de leur vie privée, sans que les pouvoirs publics disposent de réels moyens de coercition.

Cette impuissance des gouvernements à mettre en place une législation mondiale coercitive a conduit des associations de la société civile et des experts en protection de la vie privée de 40 pays à publier une déclaration en 2009. Celle-ci exigeait des gouvernements qu'ils mettent en place et fassent appliquer une législation efficace en matière de respect de la vie privée.[16]

COMMENT SE PROTEGER?

La protection de la vie privée sur Internet en général et sur les réseaux sociaux en particulier devient de plus en plus indispensable. La vigilance reste le fer de lance de la sécurité et donc de la confidentialité des informations. Elle peut se décliner en quelques techniques simples mais susceptibles de faire toute la différence:

- **Choix des "amis" et interlocuteurs**—Il convient d'être extrêmement prudent dans le choix de ses amis sur ces réseaux. Une pratique courante consiste à accepter d'entrer en contact avec les amis de nos amis, de parfaits inconnus pour la plupart. Cela peut conduire à exposer s'intimité à des personnes potentiellement nuisibles.
- **Restriction des contenus privés aux seuls proches**—De plus en plus, les sites de réseautage social permettent à leurs utilisateurs de configurer les restrictions d'accès à leurs données. Il est donc important de les exploiter et de s'assurer de la bonne configuration de ces restrictions, vu que par défaut, nos informations sont publiques.
- **Choix minutieux des informations à diffuser**—La clé de la protection de la vie privée réside en effet dans les informations à diffuser. Nom, prénom, date de naissance, lieu de naissance, photos, vidéos, commentaires et opinions doivent être minutieusement sélectionnées avant d'être postés. Garder à l'esprit qu'une information postée sur un réseau est susceptible, un jour ou un autre, de se retourner contre son auteur.
- **Sensibilisation**—Chaque tranche de la population doit être sensibilisée sur la nécessité de se protéger contre le risque que peuvent entraîner l'utilisation des réseaux sociaux. Dans le monde de l'entreprise, cette sensibilisation doit impérativement faire partie du programme de sécurité informatique.

CONCLUSION

Les réseaux sociaux sont un formidable moyen de s'exprimer et d'échanger avec les autres. Ils permettent de lever les barrières spatio-temporelles et de communiquer avec le monde entier. Cependant, il existe un revers lié aux dangers avérés de violation de la vie privée des utilisateurs.

Ces dangers sont d'autant plus menaçants qu'une tendance prend de plus en plus d'ampleur: celle de s'enregistrer sur plusieurs sites à l'aide d'un seul et unique compte d'utilisateur. Face à cette situation, chaque Internaute doit rester vigilant et les pouvoirs publics exercer davantage de pressions sur les éditeurs de ces sites afin de préserver la sécurité des Internautes.

NOTES DE FIN

1 Creative Commons, 2011, *http://controverses.ensmp.fr/wordpress/promo10g20/importance-des-reseaux-sociaux/*

2 Hempel, Jessi; "How LinkedIn will fire up your career," CNN, 25 Mars 2010, *http://money.cnn.com/2010/03/24/technology/linkedin_social_networking.fortune/*

3 Boyd, Danah; Eszter Hargittai; "Facebook Privacy Settings: Who cares?", *First Monday*, vol. 15, August 2010, *http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589*

4 Bardy, Genaro; "Etude deloitte state of the media democracy," 5 Avril 2011, *www.slideshare.net/genarobardy/etude-deloitte-state-of-the-media-democracy*

5 *Journal Le Monde*, 28 Mai 2010, p. 16

6 Commission Nationale de l'Informatique et des Libertés (CNIL), France, "L'usurpation d'identité en questions," 17 Mars 2011, *www.cnil.fr/vos-libertes/vos-droits/details/article/lusurpation-didentite-en-questions/*

7 Action Innocence, Suisse, 28 Février 2008, *www.actioninnocence.org/suisse/Fichiers/ModeleContenu/216/Fichiers/myspaceinfo.pdf*

8 Balagué, Christine; David Fayon, "Facebook, Twitter et les autres...," Edition Pearson Village Mondial, 26 Février 2010

9 Journal du Net, «Facebook va réaliser 4 milliards de dollars de CA publicitaire en 2011,» 1 Décembre 2011, *www.journaldunet.com/ebusiness/le-net/facebook-va-realiser-4-milliards-de-dollars-1211.shtml*

10 Rédaction de 01net,"Spams pornographiques : Facebook enquête," 16 Novembre 2011, *www.01net.com/editorial/546568/epidemie-d-and-039-images-pornos-facebook-enquete/*

11 Manjoo, Farhad; "De plus en plus difficile de mentir à ses proches sur Facebook," 4 Octobre 2010, *www.slate.fr/story/26401/mentir-facebook-places*

12 Le Bourlout, Eric; "Comment obtenir Timeline, le nouveau profil Facebook," 23 Septembre 2011, *www.01net.com/editorial/541884/comment-obtenir-timeline-le-nouveau-profil-facebook /*

13 Entretien avec Christophe Alix, Ecrans.fr, le 19 Février 2009, *www.ldh-toulon.net/spip.php?article3142*

14 Perret, Jean; "Article sur la législation des réseaux sociaux en Europe," 4 Mai 2011, *www.inaglobal.fr/droit/article/sur-la-legislation-des-reseaux-sociaux-en-europe*

15 Rédaction Arobasenet, "Facebook sévèrement taclé par la FTC," 1 Décembre 2011, *www.arobasenet.com/2011/12/facebook-face-a-ses-responsabilites-par-la-ftc/*

16 "Déclaration de la société civile présentée par la coalition internationale 'The Public Voice'," Madrid, 3 Novembre 2009, *www.ldh-toulon.net/spip.php?article3590*

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

www.isaca.org