Protection de la Vie Privée dans les Réseaux Sociaux d'Entreprise

Lazhar Khelifi, Fodé Touré, Esma Aïmeur

Département d'Informatique et de Recherche Opérationnelle (DIRO), Université de Montréal,Pavillon André-Aisenstadt, DIRO CP 6128 succursale Centre-Ville Montréal QC H3C3J7,Canada.
{khelifil,tourefod,aimeur}@iro.umontreal.ca

Editeur: Rapport Technique de DIRO n° 1369

RÉSUMÉ. Le réseau social d'entreprise est un outil de partage qui favorise les échanges entre les employés en leur permettant de stocker, de partager, de rendre disponible virtuellement des dossiers et de réaliser un travail d'équipe en temps réel ou différé. Ainsi, les entreprises utilisent les réseaux sociaux pour améliorer la rentabilité de leurs services. Elles ont le choix entre les réseaux sociaux internes qui permettent le partage de connaissances et d'informations (Yammer, Jamespot, etc.) et les réseaux sociaux ouverts qui permettent aux entreprises de présenter leurs produits (Google+, Viadeo, Facebook, etc.).
Les réseaux sociaux d'entreprise accroissent l'efficacité du système d'information. Ainsi, le système de gestion de la relation client en est un bel exemple. En effet, la gestion de la relation client (Customer Relationship Management- CRM) intègre les échanges internes à l'entreprise pour une meilleure efficacité. En utilisant les réseaux sociaux d'entreprises, cet outil synchronise l'ensemble des données des employés concernant les prospects, les clients et l'avancée des projets. Il gère donc les informations internes et externes de l'entreprise.
Bien que ces réseaux sociaux possèdent beaucoup d'avantages, ils soulèvent des problèmes de vie privée pour les clients et de confidentialité pour l'entreprise elle-même.
Dans cet article nous présentons les problèmes de vie privée dans les réseaux sociaux d'entreprise. Nous faisons l'état de l'art des solutions de protection de la vie privée dans ces réseaux. Nous citons les lois qui régissent la collecte et le traitement de données dans ces réseaux et nous proposons un système tiers de protection de vie privée entre le réseau social d'entreprise et le système d'information.

ABSTRACT. The enterprise social network is a sharing tool that promotes exchanges between employees allowing them to store, share and make available virtual folders, and to realize team work in real time or in an asynchronous manner. Thus, companies use social networks to improve the profitability of their services. They have the choice between internal social networks allowing the sharing of knowledge and information (Yammer, Jamespot...) and open social networks allowing company to showcase its products (Google+, Viadeo, Facebook ...).These open social networks promote interaction with customers.
Enterprise social networks increase the efficiency of the information system. For instance, the system of Customer Relationship Management (CRM) is a good example. Indeed, the CRM integrates the internal exchanges in the company for better efficiency. By using enterprise

social networks, this tool synchronizes all employees data concerning prospects, customers and project progress, and so on. Therefore, it manages the internal and external information of the enterprise.
Although these social networks have many advantages, they raise serious privacy issues for customers and the company itself.
In this paper, we present the privacy issues in enterprise social networks. In particular, we review the state of the art of solutions for privacy protection in social networks of enterprise. We quote the laws that govern the collection and processing of data in these networks and we propose a middleware for privacy protection between the enterprise social network and the information system.

MOTS-CLES : Système d'information, Réseaux sociaux d'entreprise, Vie privée, Sécurité.

KEYWORDS: Information System, Enterprise social network, Privacy, Security.

1. Introduction

Les réseaux sociaux constituent un marché de premier plan, qui ne peut être ignoré par les entreprises. Elles ont rapidement compris l'importance d'utiliser les réseaux sociaux, à des fins financières et pour gérer leur e-réputation (Lauras, 2013). Certaines entreprises ont décidé de les utiliser à des fins professionnelles, afin de faire participer leurs employés et leurs clients à la vie de l'entreprise. Ainsi, les collaborateurs (employés et clients) ne sont plus de simples consommateurs d'informations, mais deviennent également des contributeurs proactifs.

Le Réseau Social d'Entreprise (RSE) soutient l'innovation et le bon fonctionnement des Systèmes d'Information (SI). En effet, le RSE traite des personnes, mais aussi du contenu, il est donc crucial qu'il se lie avec les systèmes d'information. L'autre dimension, moins évidente est celle de la socialisation des applications d'affaires. Il s'agit de donner une vision «sociale » aux actions qui ne le sont pas (Garnier et Hervier, 2011a).

Beaucoup d'organisations ont déjà intégré un réseau social d'entreprise au cœur de leur fonctionnement et leur nombre ne fait qu'augmenter chaque année. Une étude menée en 2012 par le cabinet McKinsey sur 4200 utilisateurs de réseaux sociaux d'entreprise montre que 20% des utilisateurs de RSE se servent de cet outil dans le cadre de leur processus de veille technologique (Figure 1).

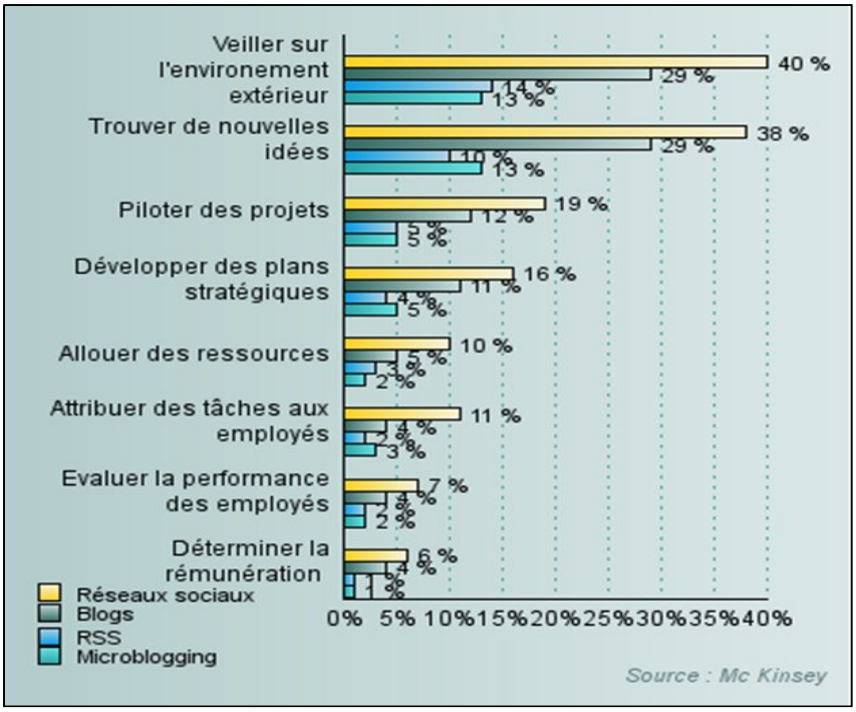

Figure 1. Usage des outils sociaux en entreprise (McKinsey, 2012).

Il existe quatre grandes composantes d'intégration des réseaux sociaux d'entreprise: la *gestion des utilisateurs*, les *applications informationnelles* (courriel, intranet, bureautique), les *applications d'affaires* (*Enterprise Resource Planning* - ERP, *Customer Relationship Management* - CRM) et enfin l'*externe* dont le site Web mais aussi les autres SI externes. Chaque cas d'usage délimitera les besoins en termes d'affaire, tandis que l'intégration dépend de l'avancement et du choix en termes de SI.

Le RSE ne remplace pas les solutions d'affaires telles que l'emailing marketing, le CRM, le support client ou la gestion de la comptabilité. Il propose d'organiser la communication interne de l'entreprise pour avoir une vue globale sur l'ensemble des entités et des projets. Le RSE facilite les échanges, centralise les données, partage les ressources, organise les projets, et héberge les documents de manière centralisée (Cholet, 2012). Par conséquent, le RSE est une extension des applications existantes, et pour ce faire il doit être intégré à l'existant, à la fois en termes de processus mais aussi technique.

On distingue deux types de réseaux sociaux d'entreprise :les *réseaux internes* et les *réseaux ouverts*. Les réseaux sociaux internes, tels que *Yammer* et *Jamespot*,

permettent le partage des connaissances et d'informations entre les employés au sein de l'entreprise, tandis que les réseaux sociaux ouverts, tels que *Google+*, *Viadeo* et *Facebook*, permettent à l'entreprise de présenter ses produits et services aux clients. Ce type de réseaux sociaux est considéré comme un outil de promotion et de marketing qui permet d'une part à l'entreprise de suivre le marché et de réagir rapidement face aux changements et d'autre part de fournir de l'information pertinente à ses utilisateurs (clients et employés).

Malgré les avantages qu'ils offrent, ces réseaux soulèvent des problèmes majeurs de *vie privée* pour les utilisateurs et de sécurité pour le système d'information. En effet, le modèle économique des réseaux sociaux est principalement basé sur la constitution de bases de données gigantesques, sur les utilisateurs, pour lesquelles les entreprises et agences gouvernementales sont prêtes à payer beaucoup d'argent. Dans ce contexte, il est évident que le respect de la vie privée n'est pas la première préoccupation des éditeurs de ces sites. Ceux-ci créent des applications potentiellement dangereuses pour la protection de la vie privée, et qui sont parfois installées par défaut sur chaque profil. L'illustration de cet état de fait est par exemple un système de *géolocalisation* qui collecte les données géographique de l'utilisateur à partir de son adresse IP, ou encore de *Timeline*, qui génère une sorte de biographie de l'utilisateur avec l'ensemble de ses publications (interactions).

Dans le RSE, les dangers augmentent car les victimes sont à la fois dans l'entreprise et hors de celle-ci. En fait, les entreprises sont conscientes du danger de divulgation, tant accidentelle que volontaire, d'informations à l'extérieur par les employés. Cette situation peut conduire à la violation de la vie privée des employés et des clients. En outre, les mesures minimales de sécurité ne sont pas toujours mises en œuvre pour protéger les données lors de leur collecte ou lors de leur conservation (Piolle, 2009). Cela peut permettre à des personnes non autorisées d'attaquer ces systèmes et d'accéder à des données parfois très sensibles (comme des informations bancaires).

Néanmoins, de nombreux outils ont été proposés pour protéger la vie privée et les données personnelles des utilisateurs et afin d'assurer la sécurité des réseaux sociaux d'entreprise.
Dans cet article, nous présentons une revue de littérature sur la protection de la vie privée dans les réseaux sociaux d'entreprise et sa relation avec le système d'information de l'entreprise. Tout d'abord, dans la section 2, nous rappelons les concepts liés aux réseaux sociaux. Ensuite, nous expliquons, dans la section 3, comment les réseaux sociaux s'intègrent dans le système d'information de l'entreprise. Etant donné que ces réseaux créent des problèmes de vie privée, nous abordons les principes fondamentaux de la protection de la vie privée dans la section 4. Nous parlerons des solutions techniques et réglementaires qui garantissent la sécurité des données des employés et des clients dans ces réseaux. Dans la section 5, nous discutons quelques principes de respect de vie privée, nous proposons un système tiers de protection de vie privée entre le réseau social d'entreprise et le système d'information. Nous terminons ce travail par une conclusion à la section 6.

2. Réseaux sociaux

Les réseaux sociaux nous permettent de rester en contact avec nos amis, de partager avec eux des informations grâce aux outils d'interaction qu'ils fournissent. Dans cette section, nous définissons et présentons l'évolution des réseaux sociaux.

2.1. Définition

C'est en 1954 que John Barnes, un sociologue, dans son article « *Class and Committees in a Norwegian Island Parish*» a donné un cadre méthodologique à la compréhension des réseaux sociaux (Barnes, 1954). Il les a définis comme étant des « *relations et des flux entre des personnes, des groupes, des organisations, des animaux, des ordinateurs ou d'autres entités d'informations / connaissances traitées* ».

Selon Fogel et Nehmad (2009), les réseaux sociaux sont des espaces sociaux sur Internet permettant le partage d'informations, la communication et la collaboration entre divers acteurs. De plus, un réseau social repose sur trois composantes principales : le *profil de l'utilisateur* (publication d'informations personnelles), l'*établissement d'un cercle d'amis* (création de listes et sous-listes selon des intérêts communs) et l'*interaction entre utilisateurs* (échange d'informations).

Boyd et Ellison(2007) définissent les sites de réseaux sociaux en tant que services Web qui permettent aux individus de (1) construire un profil public ou semi-public dans un système borné, (2) d'articuler une liste d'autres utilisateurs avec lesquels ils partagent une connexion, et (3) de voir et parcourir leurs listes de connexions et celles des autres au sein du système. La nature et la nomenclature de ces connexions peuvent varier d'un site à un autre.

Selon Aïmeur et *al. (2010)*, les sites de réseaux sociaux sont des sites web qui permettent aux utilisateurs de :

- Communiquer avec d'autres utilisateurs par «*befriending*» (Facebook), par partisans (Twitter), par abonnement (YouTube);
- Interagir avec le contenu posté par d'autres utilisateurs, par exemple en commentant, en répondant ou par notation;
- Restreindre leur propre contenu aux seuls utilisateurs autorisés.

2.2. Historique

Boyd et Ellison (2007) ont étudié l'historique et l'évolution des réseaux sociaux jusqu'à l'année 2007. D'après ces auteurs, le premier réseau social lancé en 1997 est *SixDegrees.com*. Il permettait déjà à l'utilisateur de créer un profil et de lister ses amis. Malheureusement ce réseau a rencontré des difficultés qui ont causé sa fermeture en 2008 malgré ses millions d'utilisateurs.

Plusieurs sites de réseaux sociaux sont apparus entre l'année 1997 et l'année 2000, combinant les profils et les listes d'amis (par exemple *MiGente et AsianAvenue*). L'année 2001est caractérisée par les premières ébauches d'une nouvelle vague de réseaux sociaux : les *réseaux professionnels*. C'est dans ce contexteque le réseau social *Ryse.com* est apparu. D'autres réseaux sociaux professionnels comme *Tribe.net*, *Friendster* et *Linkedln* ont également été développés. Mais même avec du soutien et des investissements, *Ryse et Friendster* n'ont pas eu le sucées compté, seul *LinkedIn* est devenu puissant dans ce domaine.

L'année 2003 a vu l'apparition de plusieurs nouveaux réseaux sociaux. La plupart d'entre eux ont essayé de rivaliser avec *Friendster*, en ciblant un sujet particulier tel que l'origine démographique des utilisateurs, les intérêts communs entre les utilisateurs, les associations caritatives ou même la religion pour connecter les croyants entre eux (Gandouz, 2012).

Toujours en 2003,le réseau *MySpace*a fait son entrée sur le marché et devient le numéro un des sites de réseaux sociaux. Il était connu pour héberger de nombreuses pages Internet de groupes musicaux et de musiciens qui y entreposaient et présentaient leurs compositions musicales. *Facebook* est apparu en 2004, c'était un site destiné à mettre en relation, les étudiants de Harvard. Pour y adhérer, un étudiant devait fournir son courriel *harvard.edu*. À partir de 2005, Facebook est élargi pour inclure les élèves du secondaire, les professionnels et finalement tout le monde. L'évolution la plus significative de Facebook est la possibilité pour des développeurs extérieurs de créer des applications que les utilisateurs peuvent intégrer dans leurs profils. Cette nouveauté a soulevé une nouvelle fois le problème de la sécurité dans les réseaux sociaux (Gandouz, 2012).

En 2006, *Twitter* a été fondé. Il s'agit d'un réseau d'informations en temps réel qui permet à un utilisateur d'envoyer de brefs messages appelés « tweets ». L'idée était de permettre aux utilisateurs un partage facile de leurs petits moments de vie avec leurs amis. Twitter permet de garder ses utilisateurs connectés avec les dernières histoires, idées, opinions et actualités sur des événements qui les intéressent.

L'année 2011 a vu l'apparition d'un nouveau réseau social :*Google+*. Dès sa publication, il a beaucoup fait parler de lui par les spécialistes et le grand public. Pour cause, il est conçu pour s'intégrer avec la plupart des produits Google déjà bien en avance par rapport à la concurrence.

Après avoir parcouru la liste des principaux sites de réseaux sociaux qui ont marqué l'histoire, nous présentons, dans la prochaine section, les réseaux sociaux d'entreprise.

2.3. Réseaux sociaux d'entreprise

Le modèle de communication interne de l'entreprise s'adapte, lui aussi, aux nouveaux outils utilisés par les employés et les clients. Les réseaux sociaux d'entreprise demandent une amélioration des anciens modèles : la communication

descendante et centralisée cède peu à peu la place à une communication transversale et individualisée. Le principe de réseau social d'entreprise est basé sur l'échange entre des membres répartis en groupes. L'adaptation d'un réseau social d'entreprise ne se limite pas à l'implantation d'un outil mais à une révision complète du mode de fonctionnement de l'entreprise, de sa culture et de ses valeurs. Dans cette section, nous présentons les réseaux sociaux d'entreprises et leurs impacts sur le système d'information.

2.3.1. Définition

Le réseau social d'entreprise est un outil de communication au sein d'une organisation (société, association, groupement). D'après Garnier et Hervier (2011b), le réseau social d'entreprise a fait son apparition dans la suite logique de plusieurs phénomènes parmi lesquels : l'*externalisation des services*, l'*adoption des grands principes du Web 2.0* (l'utilisateur au centre, source de valeur et co-développeur, puissance des données) et la *personnalisation de la relation client* (CRM et marketing participatif). Garnier et Hervier (2011b) ont défini le réseau social d'entreprise, ou RSE, comme *l'ensemble des individus qui participent à l'écosystème de l'entreprise et la matérialisation numérique de leurs interactions relatives à leurs activités dans le cadre de cet écosystème*. L'architecture d'un réseau social d'entreprise, proposé par Balagué et Fayon (2010), est présentée à la Figure 2.La base de chaque réseau social d'entreprise est constituée de fonctions usuelles (notification par mail, listes des liens vers des références utiles, espace de travail partagé, etc.) et de contacts (base de données des clients, carnets d'adresses).

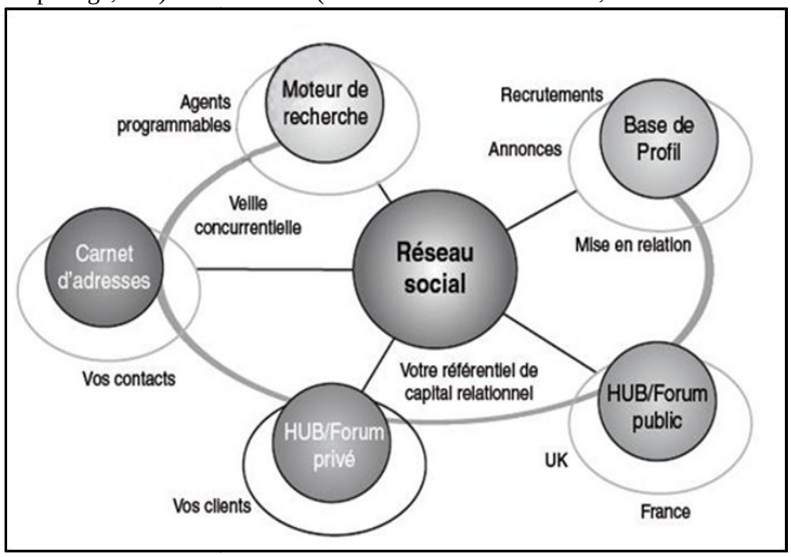

Figure 2. Architecture d'un réseau social dans une organisation (Balagué et Fayon, 2010).

2.3.2. Exemples de sites de réseaux sociaux d'entreprise

Dans cette section nous présentons les sites de réseaux sociaux ouverts comme Google+et des exemples de sites de réseaux sociaux internes comme MediaWiki, Yammer, Jamespot, BlueKiwi, etc.

Google+[1](Google Plus) est l'application de réseautage social lancée par la société Google le28 juin 2011. Elle a été accessible au grand public le 20 septembre 2011. Après avoir dépassé Twitter en janvier 2013, Google+ est le deuxième plus grand réseau social au monde. Il permet de partager de l'information aux cercles qui peuvent être internes ou externes à l'entreprise. Google+ intègre aussi les communautés qui partagent les mêmes centres d'intérêt.«*Nous intégrons dans les produits Google grand public les fonctionnalités dont votre entreprise a besoin pour atteindre ses objectifs*. » a déclaré Amit Singh le Président de Google Enterprise.

MediaWiki[2], apparu en 2004,permet à des millions d'internautes, à travers le monde, de travailler ensemble. Deux types de wikis peuvent être utilisés par une entreprise : le *wiki public* et le *wiki privé*. Le wiki public est destiné à des personnes extérieures (clients, fournisseurs). Il permet de simplifier la recherche d'informations sur votre entreprise et leur permet de s'exprimer sur vos services. Le wiki privé, appelé aussi *Intranet*, est dédié uniquement aux collaborateurs de l'entreprise. Il peut contenir des données confidentielles. Notons que, les wikis privés peuvent être fermés et, ainsi, seules les personnes autorisées y auront accès.

Yammer[3], créé en 2008,est un réseau social privé qui aide les employés d'une entreprise à collaborer à travers les ministères, les lieux et les applications. Yammer a pour but de développer l'entreprise en termes d'affaires, de stratégie et de formation. Ainsi il permet aux employés, aux gestionnaires et aux cadres de participer aux dialogues.

Chatter[4]**,** créé en 2010,par l'éditeur de logiciels *Salesforce*, permet aux équipes de se synchroniser et de collaborer en temps réel. Il permet également à tous les collaborateurs d'une même entreprise de mettre à jour leurs profils, échanger et partager tout type d'informations sur leurs activités professionnelles quotidiennes. Avec Chatter, les employés peuvent créer des actions personnalisées, déployer instantanément à chaque bureau et périphérique et accéder à n'importe quelle application.

Jamespot[5], créé en 2011, est un leader sur le marché des RSE**.** En croissance depuis sa création**,** il devient l'une des figures incontournables de l'écosystème

1. http://www.google.fr/enterprise/(Vu le 03/01/2014).
2. http://semantiki.fr/index.php/Wiki_priv%C3%A9_d'entreprise_pour_entreprise_2.0 (Vu le03/01/2014).
3. https://www.yammer.com/(Vu le 03/01/2014).
4. https://www.salesforce.com/chatter/overview/(Vu le03/01/2014).
5. http://www.jamespot.com/(Vu le 12/01/2014).

français des outils de réseaux sociaux d'entreprise. La solution Jamespot permet de connecter différents acteurs au sein de l'entreprise et à l'extérieur de celle-ci afin de partager documents, liens et articles, de les commenter et de travailler en mode projet.

BlueKiwi[6], créé en 2007,est parmi les premiers éditeurs européens de réseaux sociaux d'entreprise. BlueKiwi offre d'une part l'animation du dialogue avec l'externe via une distinction entre groupes internes et communautés externes. D'autre part, l'intégration des flux sociaux externes. Par exemple, un client interne de Twitter (API de Twitter) permet d'intégrer les conversations externes afin d'en assurer le suivi ou de préparer des réponses en interne. Il est disponible en trois éditions :*Professionnel*, *Premium* et *Entreprise*. Chaque édition est conçue pour répondre aux besoins et aux exigences des entreprises de toutes tailles.

HP Collective[7], créé en 2012, est une plateforme informatique sociale d'entreprise développée par HP Labs d'Israël. D'après HP Labs « *cette technologie élimine les silos organisationnels, y compris au sein des plus grands groupes, en fournissant aux employés un accès automatique et complet à l'ensemble du savoir de leur organisation*». Avec cette plateforme, chaque employé dispose d'un accès complet à la totalité de la connaissance de l'organisation. Un utilisateur peut identifier des experts, découvrir des contenus publiés et des analyses relatives aux sujets sur lesquels il travaille de manière simple et rapide.

Après l'apparition de sites de réseaux sociaux d'entreprise une question s'impose à savoir : Quelle est la relation entre le système d'information et les sites de réseaux sociaux ? La section suivante tente de répondre à cette question.

3. Réseaux sociaux: une composante de Système d'Information de l'entreprise

Avec l'utilisation combinée de moyens informatiques, électroniques et d'outils de télécommunication, l'entreprise devient capable d'automatiser et de dématérialiser toutes ses activités. Par conséquent, l'architecture des composants d'un système d'information se modifie dans le sens où d'autres composants peuvent être inclus pour offrir des caractéristiques techniques ou des fonctionnalités spécifiques. Dans la Figure 3, nous présentons une architecture de système d'information en tenant compte de l'utilisation de sites de réseaux sociaux.

6. http://www.bluekiwi-software.com/fr/entreprise/ (Vu le 14/01/2014).
7. http://www.decideo.ca/Graphes-sociaux-pour-entreprise-le-projet-HP-Collective demontre- la-puissance-des-reseaux-sociaux-d-entreprise_a5216.html (Vu le 16/01/2014).

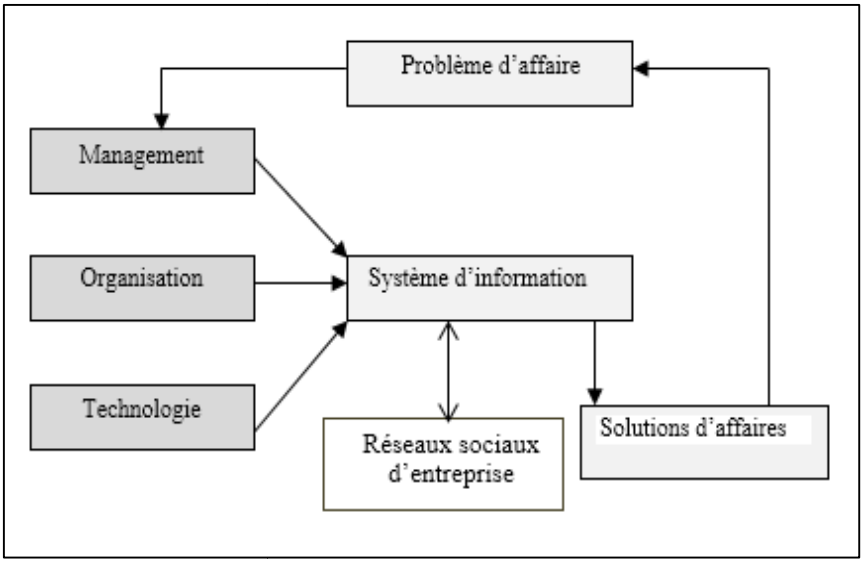

Figure 3. Architecture de système d'entreprise. Cette figure est adaptée de Laudon et Laudon (2013).

Tous les secteurs sont touchés par ces réseaux. «*Que l'on soit dans un bureau ou sur une chaîne de montage, ces outils se montrent utiles dans tous les cas où les salariés doivent résoudre des exceptions, au travers de nouvelles approches … On avait pensé que le RSE allait remplacer l'email, la gestion de processus d'affaire (Business Process Management - BPM) ou la gestion de contenu d'entreprise (Enterprise Content Management - ECM). Il faut en fait le connecter à ces outils, ainsi qu'à l'ERP, le CRM, le Case Management et la gestion de projets … De même, l'annuaire RH, le calendrier ou la gestion de projets pourrait être directement accessible dans le RSE*», explique Bertrand Duperrin, consultant chez Next Modernity. Le RSE offre une connectivité croissante vers les autres applications du système d'information de l'entreprise. Il s'agit par exemple d'injecter dans le flux social, des événements générés par les outils d'affaires. Ainsi, un retard sur le prévisionnel génèrera une alerte dans le RSE, à partir duquel on pourra directement réagir, car le composant SAP concerné sera intégré dans l'interface du RSE.

Dans la section 3.1, nous présentons les avantages liées à l'utilisation des réseaux d'entreprise.

3.1.Avantages de sites de réseaux sociaux d'entreprise

Les réseaux sociaux d'entreprise donnent plus en termes de gain de productivité et de connectivité. Ces nouveaux espaces d'échanges séduisent les entreprises du fait de leur capacité à générer de l'intelligence collective, à faciliter le travail collaboratif (Cross et *al.*,2000) et à favoriser l'innovation (Deltour et *al.*, 2011). Aussi, la nature dynamique des réseaux sociaux permet des communications assez rapides et faciles entre les employés.Une étude récente de Dorris (2014) montre que l'utilisation des médias sociaux profite à l'organisation dans la mesure où ils permettent d'influencer le comportement des clients.

Avec un tel réseau, les employés d'une entreprise sont capables de créer des groupes de travail thématiques, de communiquer au sein des équipes et de partager des informations et des documents d'une manière plus efficace. L'utilisation des réseaux sociaux permet aussi au personnel d'une entreprise d'éviter les déplacements pour rencontrer des collègues ou des clients, d'envoyer et lire moins de courriels et de limiter les réunions internes. Comme autre avantage d'utilisation de sites de réseaux sociaux nous pouvons citer le sondage en ligne. En effet, l'entreprise n'est pas obligée d'investir dans d'autres outils pour vérifier la satisfaction de ces clients. En outre, l'entreprise gagne de nouvelles opportunités[8]qui lui permettent de :

- Rester dans la boucle des nouveaux développements;
- Comparer les produits et les services;
- Suivre les opportunités commerciales;
- Garder un œil sur les offres d'emploi;
- Identifier des experts ou des contributeurs invisibles dans l'entreprise;
- Faciliter le travail en commun;
- Renforcer la cohésion d'équipe;
- Faciliter la prise de décision.

Selon Pellerin (2011), les réseaux sociaux d'entreprise créent de nouveaux postes hiérarchiques et permettent de modifier les responsabilités dans différents départements de l'entreprise (souvent le département marketing). Ces postes sont:

- *Gestionnaire de médias sociaux* : il est responsable de la construction et de l'optimisation des stratégies social-média, de la gestion quotidienne de toutes les plateformes de médias sociaux, de la surveillance et du suivi de l'efficacité de ceux-ci;
- *Coordinateur de communications numériques* : il est chargé d'entretenir régulièrement le site Internet de l'entreprise et est responsable de la communication sur les réseaux sociaux;
- *Développeur d'applications sociales* : il est chargé de diriger tous les aspects du développement d'applications sociales à travers les

8. http://www.communication-web.net/2011/06/14/ce-que-changent-les-reseaux-sociaux-d%E2%80%99entreprise-12/ (Vu le06/01/2014).

communautés de l'entreprise. Il s'agit de la personne qui aura le plus d'affinités avec les plates-formes sociales telles que Facebook, Twitter, etc.;

– *Spécialiste de référencement Web* : il réalise des campagnes de référencement et d'actions sur les réseaux sociaux ;

– *Gestionnaire de contenu Web* : il est chargé de produire un contenu régulier pour la marque afin d'entretenir la relation avec les internautes.

Bien que les sites de réseaux sociaux offrent des nouvelles opportunités aux entreprises, ils ont aussi des inconvénients qui touchent tous les acteurs au sein de l'entreprise. Dans ce contexte, l'étude faite par Kin Chan et Virkki (2014) sur un nombre d'utilisateurs de réseaux sociaux montre que ces derniers voient l'Internet comme une partie du monde réel (le réseautage social est un quotidien). Les données sont autant sensibles sur les réseaux sociaux que dans le monde réel.
La section 3.2 présente les dangers de l'utilisation des réseaux sociaux d'entreprise.

3.2. Dangers dus aux sites de réseaux sociaux d'entreprise

Les réseaux sociaux créent des problèmes de sécurité pour l'entreprise et ses clients, en raison du caractère personnel et sensible des données qu'ils collectent et traitent. En effet, l'interaction en ligne et le partage de renseignements personnels sur les sites en ligne ont soulevé de nombreux problèmes de bris de la vie privée car ces outils fournissent une quantité de données personnels énorme, qui peut être utilisée à mauvais escient par des activités malveillantes contre la volonté de l'utilisateur (Dhawan et Geol, 2014).Comme exemple de données personnelles nous pouvons citer : le nombre d'amis sur un réseau social, les messages et la liste des contacts. De plus, il arrive que l'employeur demande aux futurs employés leurs identifiants de connexion (Lafond et *al.*, 2012). C'est pour cette raison que les utilisateurs de réseaux sociaux d'entreprise sont de plus en plus hostiles au fait de divulguer leurs informations, car ils sont conscient de leurs vies privées (Herder et Kawase, 2012; Bouget, 2013).
Dans cette section, nous présentons quelques dangers liés aux réseaux sociaux d'entreprise ainsi que ses effets néfastes sur les différents acteurs au sien de l'entreprise.

3.2.1. Vol d'identité

Alors que l'informatique et les technologies numériques s'immiscent dans la vie des utilisateurs et souvent à leur insu, les risques d'attaques et plus précisément ceux liés au vol d'identité se multiplient (Dupont et Aïmeur, 2010). Le vol d'identité, connu aussi sous le nom d'*usurpation d'identité*, est le fait de voler l'identité d'une autre personne vivante et d'acquérir des renseignements signalétiques sur elle, généralement, dans le but de réaliser des actions frauduleuses en son nom. Le vol d'identité n'est pas un problème banal, il connaît une croissance rapide et il peut

toucher un client, un employé ou une entreprise. Il provoque la perte de confiance entre ces trois acteurs (client, employé, entreprise), ce qui peut provoquer un grand problème pour l'entreprise.«*L'objectif du vol d'identité en entreprise peut être d'atteindre l'infrastructure TI, de commettre une fraude, de faire de l'espionnage industriel ou de vendre les informations recueillies à des publicitaires qui vous bombarderont ensuite de courriels non sollicité*s.», déclare Jean Loup Le Roux, conseiller principal en sécurité de l'information chez In Fidem[9].

Le vol de l'identité d'un employé de l'entreprise peut aussi déstabiliser le système d'information et affecter une propriété très importante : la *transparence*. Selon Dominique Plasse, conseiller technique chez FortiNet[10], « *il est plus aisé d'agir au nom d'un employé pour pénétrer un système informatique d'entreprise que de profiter d'une brèche de sécurité pour laquelle il n'existe pas encore de rustine*».

3.2.2. Hameçonnage

« *Le mot hameçonnage vient de l'analogie que les fraudeurs sur Internet utilisent des courriels appâts pour aller à la pêche aux mots de passe et aux données financières dans la mer des utilisateurs d'Internet*»[11].Avec la croissance de l'utilisation de réseaux sociaux par les entreprises, l'hameçonnage, parfois appelé *phishing*[12],devient une technique très utilisée par des fraudeurs, dans le but d'avoir des informations spécifiques telles que :*mot de passe, numéro de compte bancaire* d'une entité qu'elle soit une personne ou une entreprise. La technique est de faire croire à la victime qu'elle s'adresse à un tiers de confiance vers l'entreprise (banque, administration, etc…).

3.2.3. Profilage

Le principe du profilage repose sur le recueil d'informations à partir d'un certain nombre de ressources. Avec les réseaux sociaux, les entreprises sont capables de construire des profils complets sur les clients actuels et même sur les futurs clients afin de leur vendre des produits sur la base de leur comportement. Ceci est souvent effectué sans que la personne ne sache ce qui se passe derrière l'interface de ce réseau et sans lui donner la chance de se retirer du processus de création de dossier (Aïmeur *et al.*, 2010).

Vu que les utilisateurs ne connaissent pas les inconvénients des réseaux sociaux d'entreprises et ses influences qui sont parfois graves, il est facile pour l'entreprise

9. http://www.infidem.biz/(Vu le06/01/2014).

10. http://www.fortinet.com/ (Vu le 06/01/2014).

11. http://www.antifraudcentrecentreantifraude.ca/francais/recognizeit_phishingemails.html (Vu le06/01/2014).

12. http://www.caprioli-avocats.com/pdf/securite-informatique2.pdf(Vu le 08/01/2014).

de télécharger de nombreux renseignements personnels, tels que l'*âge*, le *numéro de téléphone*, l'*adresse à domicile*, des *photos* et même l'*orientation sexuelle* d'un client. Ces informations peuvent être utilisées plus tard par l'entreprise pour des fins de marketing.

3.2.4. Cyber intimidation

Smith *et al.,* (2008) ont défini la cyber intimidation comme étant « *un acte agressif et intentionnel commis par un groupe ou un individu, en utilisant des formes de communication électroniques, de façon répétée et sur une personne qui ne peut se défendre facilement* ». Dans ce contexte, les réseaux sociaux d'entreprise peuvent être utilisés à mauvais escient pour harceler ou humilier les employés ou les clients. Il s'agit certainement d'un gros risque chez les employés et les clients, car cela peut les amener à se sous-estimer, à devenir anxieux, dépressifs et violents et peut même les pousser au suicide (Gandouz, 2012).La diffusion d'une vidéo personnelle d'un employé sur le réseau social dans un premier temps et le chantage de cette victime dans un deuxième temps est un exemple d'acte de cyber intimidation.

3.2.5. Concurrence déloyale

La concurrence déloyale est connue de longue date entre les entreprises sur le marché mondial, mais l'apparition des réseaux sociaux d'entreprise a exacerbé le problème. Aujourd'hui, les réseaux sociaux peuvent permettre à toute personne d'apprendre des informations et des connaissances concernant l'entreprise ou même les employés. En outre, il est possible qu'un employé traite secrètement des informations confidentielles avec un concurrent sur le web. Par conséquent, il peut parler librement sur les secrets commerciaux et même critiquer les orientations de son entreprise (Lafond *et al.*, 2012).Ainsi, les entreprises peuvent s'espionner mutuellement à l'aide de ce flux d'informations et de messages qui circulent dans les réseaux sociaux.

3.2.6. E-réputation

La réputation est l'évaluation sociale du public envers une personne, un groupe de personnes ou une organisation(Aïmeur *et al.,* 2010). Il s'agit d'un facteur important dans de nombreux domaines tels que les affaires, les communautés en ligne ou statut social (Dingledine *et al.*, 2003).

Le terme e-réputation est en relation avec l'apparition de web 2.0.Rosa et Garry (2001), ont étudié ce problème. L'e-réputation, appelée aussi *cyber-réputation* ou *web-réputation*, devient un problème crucial avec l'apparition de réseaux sociaux d'entreprise. Par exemple, «*cinq infirmières du Centre Médical de Tri City à San Diego et au Ministère de la Santé de la Californie ont été renvoyées (retraite anticipée) après qu'il ait été découvert que leurs conversations publiques en ligne incluaient des informations privées sur des cas de patients, ce qui est une violation du droit à la vie privée* » (Stickney, 2010; Lafond *et al.*, 2012).L'e-réputation provoque des pertes financières importantes pour l'entreprise .Ce problème occupe

le premier rang, au-dessus de la perte de données, le vol du droit d'auteur et les pertes financières.

Dans la section suivante nous présentons les principes fondamentaux de la protection de la vie privée dans les réseaux sociaux .

4. Protection de la vie privée dans les réseaux sociaux d'entreprise: principes fondamentaux

La protection de la vie privée est un droit fondamental. La vie privée est protégée au niveau international par l'article 12 de la Déclaration Universelle des Droits de l'Homme :(*a) Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni ne sera l'objet d'atteintes à son honneur et à sa* réputation. *(b) Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* Pour qu'elle respecte cet article, la protection de la vie privée dans les réseaux sociaux d'entreprise doit considérer quelques principes fondamentaux. Ces principes garantissent le droit fondamental à la protection de la vie privée des personnes et déterminent en même temps les obligations des entreprises. Plusieurs travaux, dans la littérature, ont spécifié les propriétés et les principes qu'un système doit avoir pour préserver la vie privée de l'utilisateur. Nous pouvons citer les travaux de Kobsa (2007) et de Wang et Kobsa (2006) qui ont étudié les lois et les règlements de protection de la vie privée et la littérature dans le domaine de la sécurité et les systèmes personnalisés afin de formuler ces propriétés. En outre, Wicker et Schrader(2011) ont travaillé sur la protection de la vie privée dans les réseaux d'informations. En nous basant sur ces travaux, nous détaillons quelques principes fondamentaux.

4.1. Minimisation des données personnelles

Le principe de minimisation des données indique que seules les informations nécessaires, pour compléter une application particulière, devraient être divulguées (et pas plus). En pratique, cela veut dire qu'il ne faut transmettre les informations qu'à ceux qui en ont besoin, tout en respectant le principe de confiance (Aïmeur *et al.*, 2010). Ce principe de minimisation est une conséquence de l'application directe des critères de légitimité définis par la Commission européenne sur la protection des données[13].

4.2. Souveraineté sur les données personnelles

Les résultats indiqués dans une étude de Wang et Kobsa (2006) montrent que 69% des utilisateurs des réseaux sociaux pensent qu'avoir le contrôle et la

13.La directive 95/46/CE du Parlement européen et du Conseil relative à la protection des données à caractère personnel et à la libre circulation de ces données, 1995.

souveraineté sur leurs données personnelles après la collecte est très important et 24% des participants trouvent cela assez important. Ces résultats suggèrent que le système doit être en mesure d'informer les utilisateurs de la quantité de données collectées. Les utilisateurs devraient également connaitre les raisons de la collecte de leurs données et leurs utilisations. Selon Deswarte et Gambs (2010), le principe de souveraineté couvre l'exigence de « consentement libre et éclairé » qui suppose que la personne soit avertie de l'usage qui sera fait des données personnelles qu'elle confie et qu'elle y donne son accord.

4.3. Consentement explicite

D'après le site de commissariat à la protection de la vie privée du Canada, selon le principe de consentement, les personnes doivent être informées de toute collecte, de toute utilisation ou communication de renseignements personnels qui les concernent et y consentir. Il s'agit un accord, exprimé par le propriétaire des données, permettant la collecte et le traitement de ses données personnelles. Dans la législation européenne, on considère que l'utilisateur n'autorise pas le traitement (Deswarte et Gambs, 2010). Bien évidemment, les textes légaux prévoient des exceptions dans les cas mettant en jeu la santé publique, la sécurité nationale ou l'instruction d'affaires judiciaires (Deswarte et Gambs, 2010).

4.4. Transparence

Selon Walter (2012), «*il s'agit tout d'abord de renforcer la transparence des traitements en prévoyant l'information des personnes concernées de la collecte de données peu importe la nature des données et quel que soit l'organe, la personne ou l'entité qui procède à la collecte de ces données*». L'information doit être complète et accessible pour donner aux utilisateurs la possibilité de réagir. De plus, l'information doit être délivrée de manière intelligible et doit être simple et claire.

4.5. Imputabilité

Le principe d'imputabilité suppose que l'entité qui héberge les données personnelles doit être sécurisée au meilleur de ses moyens, et le cas échéant peut être tenue responsable (par exemple devant un juge) d'un bris de vie privée si elle manque à ses obligations. Ce principe est nommé parfois gestion de la preuve (Deswarte et Gambs, 2010). Selon la commission de la protection de la vie privée de Belgique[14], l'imputabilité assure le pouvoir d'identifier toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder la trace de l'auteur et de l'action (traçabilité).

14. http://www.privacycommission.be/sites/privacycommission/files.pdf(Vu le06/01/2014).

4.6. Sécurité des données

L'entreprise doit implémenter des mécanismes et utiliser des mesures de sécurité pour protéger les données des utilisateurs contre tout accès illégal, divulgation, reproduction, modification ou toute utilisation inappropriée. Ces mécanismes doivent correspondre aux degrés de sensibilité des informations personnelles. Donc, il est primordial de mettre en place des mécanismes de contrôle d'accès qui gèrent l'accès aux données de l'utilisateur et des mécanismes cryptographiques pour assurer les deux propriétés de la sécurité à savoir : la *confidentialité* et l'*intégrité*.

Pour que ces différents principes soient respectés il faut des outils. Dans ce contexte beaucoup de chercheurs, dans le domaine de protection de la vie privée, se sont intéressés à l'implémentation de technologies respectueuses de la vie privée. Ces technologies ont un impact positif au niveau de la limitation de diffusion de données privées. Cependant, elles ne garantissent pas une protection totale des données personnelles. Nous discutons quelques aspects de protection de la vie privée dans la section suivante.

5. Discussion

L'utilisation des nouvelles technologies de protection de la vie privée dans les réseaux sociaux d'entreprise peut diminuer les violations de la vie privée des employés et des clients et le nombre d'attaques sur le système d'information de l'entreprise. Dans cette section, nous montrons la place de la protection de la vie privée dans la société de l'information. Nous discutons du *droit à l'oubli* et des lois liées aux problèmes de protection de vie privée. Enfin, nous proposons un système tiers de protection des données et de la vie privée entre le réseau social d'entreprise et le système d'information.

5.1. Protection de la vie privée : une des dimensions morales du système d'information

Selon Laudon et Laudon (2007), il existe cinq dimensions morales dans la sphère de l'information: *droits et devoirs de l'information* (confidentialité), *responsabilité et contrôle*, *droits et devoirs de la propriété*, *qualité de la vie et la qualité du système*. Ces dimensions sont fortement liées aux aspects éthiques, sociaux et politiques. En effet, l'utilisation des réseaux sociaux d'entreprise touche la dimension de devoirs et droits de l'information car le respect et le droit de la protection de la vie privée supposent que chaque être humain a le droit d'exiger qu'on le laisse tranquille, qu'on ne le surveille pas et que personne (individu, entreprise) n'intervienne à son issu dans sa vie privée (Laudon et Laudon, 2012). L'intégration des réseaux sociaux, dans le système d'information, peut violer cette dimension et la surveillance des employés par leurs employeurs est un exemple typique de cette violation. Pour illustrer ce qui précède, nous rapportons une histoire publiée par Megan (Heitman, 2012) : «*Avant que je ne parte en vacances, mon patron m'a demandé de garder mon téléphone sur moi parce qu'il travaillait sur un*

projet et pourrait avoir besoin de me demander des informations. Je lui ai dit que je serais disponible, mais je savais d'emblée que je n'allais pas répondre. Il a appelé au moins 10 fois, et je n'ai jamais pris le téléphone. Quand je suis rentrée, il m'a demandé pourquoi je n'avais pas répondu, j'ai alors menti en lui disant que mon téléphone avait été volé. Il m'a regardé longuement puis il m'a dit: c'est drôle, parce que, selon votre compte Twitter, vous avez été actif toute la semaine via votre téléphone». Ceci montre bien comment les superviseurs, au sien de l'entreprise, peuvent utiliser des renseignements personnels, trouvés sur les réseaux sociaux, pour surveiller des leurs employés.

5.2. Public et privé

La plupart des utilisateurs de réseaux sociaux voudraient publier et partager de l'information. Les employées utilisant un réseau social d'entreprise n'en sont pas un cas particulier, même s'ils sont tout à fait conscients des conséquences liées à la divulgation de données sensibles. La première question qui s'impose dans ce débat est : quelles sont les informations qui doivent être considérées comme privées ou publiques? La deuxième question est : quel est l'impact d'une telle stratégie de publication dans le temps ?

Comme impact chez les utilisateurs nous trouvons le *regret*. Yang *et al.* (2011) ont étudié les regrets associés aux messages des utilisateurs sur Facebook. Ils ont constaté qu'il existe différentes causes pour lesquelles les utilisateurs regrettent les informations ou les opinions postées sur Facebook. Au début, les utilisateurs ne pensent pas à la raison d'affichage d'une information ni même les conséquences de leurs messages, ils sont dans un état de grande émotion (joie, tristesse, inquiétude) lors de la publication ou sous l'influence de l'alcool. Ainsi, ils ne prévoient pas comment leurs messages pourraient être vus et considérés par les autres utilisateurs du réseau (Aïmeur *et al.*, 2013). De plus, certains employés ont l'habitude de passer beaucoup de leur temps de travail à vérifier les mises à jour des statuts de leurs amis et à bavarder avec ces derniers sur Facebook, Twitter et autres. Ce comportement constitue une menace pour la productivité. D'une part, en termes de notoriété, les employés seront touchés émotionnellement pendant le temps qu'ils passent sur ces réseaux (durant leur période de travail) et d'autre part, en termes de confidentialité, les employés qui ne sont pas conscients de la sensibilité de certaines informations d'entreprise peuvent éventuellement les divulguer à des amis et les rendre entièrement publiques (Palo Alto Networks, 2010).

Ce genre de problèmes amène d'autres questions importantes : Est-ce que l'entreprise doit offrir la liberté totale à ses employés pour l'utilisation des réseaux sociaux professionnels ou même des sites personnels? À quel moment et comment doit-elle sévir en cas de dépassement?
Les responsabilités doivent être partagées entre l'employé et l'employeur. L'employeur se charge d'offrir les moyens de protection et les règles d'utilisation et l'employé doit les respecter.

5.3. Gouvernance

Lorsque les réseaux sociaux offrent aux membres des syndicats, de nouvelles opportunités comme la possibilité de réagir contre une entreprise en faisant des commentaires, l'entreprise peut être lésée. En effet, les messages ciblés et accessibles à tous les employés ont une influence directe sur le personnel de l'entreprise, donc sur le fonctionnement de celle-ci. Ces nouvelles opportunités peuvent remplacer les modes de réaction traditionnels telles que les manifestations ou les grèves. Ces nouveaux modes de réactions peuvent causer la divulgation d'informations sensibles ou faire passer une mauvaise image de l'entreprise aux clients. Par conséquent, l'entreprise devrait trouver des solutions aux problèmes dus à l'utilisation de réseaux sociaux plutôt que de les combattre (Berdnarz, 2011).

Parent (2010) a définit la gouvernance comme «*l'ensemble de règles que l'entreprise doit mettre en œuvre pour garantir la bonne gestion de ses efforts et pour supporter en tout temps sa vision, ses objectifs, ses outils de mesure*». La gouvernance se résume en quatre points :

- Planification : il s'agit de déterminer comment les medias sociaux servent;
- Politique: il s'agit du comportement et de l'usage des médias sociaux – qu'est ce qui peut être fait et par qui (quelle fonction), quand et comment? Qu'est ce qui est approprié et qu'est ce qui ne l'est pas ?
- Préparation: il s'agit de déterminer quel type de plateformes de médias sociaux l'entreprise pourra utiliser et quelles ressources;
- Protocole: il s'agit du moyen par lequel l'équipe responsable des médias sociaux communiquera avec le reste de l'entreprise – comment elle présentera leurs progrès, défis et problèmes?

En plus d'une bonne politique de gouvernance, les lois et les textes législatifs sont nécessaires pour agir en cas de violation de la vie privée.

5.4. Exigence réglementaire pour la protection de la vie privée sur les réseaux sociaux

Les lois et les règles sociales qui s'appliquent à la protection de la vie privée dans le monde réel ne s'appliquent pas nécessairement au monde numérique. Les lois relatives aux réseaux sociaux sont encore en cours de développement (Lafond et *al.*, 2012). Au Canada, la vie privée dans le site des réseaux sociaux est protégée par la *Loi sur la Protection des Renseignements Personnels et les Documents Electroniques* (LPRPDE) de 2001. Cette loi définit les règles applicables sur la façon dont les organisations du secteur privé peuvent recueillir, utiliser et communiquer des renseignements personnels dans le cadre d'activités commerciales. Il y a aussi le Commissariat à la protection de la vie privée qui a pour rôle d'enquêter sur les plaintes, de mener des vérifications et d'intenter des poursuites judiciaires en vertu de lois fédérales en cas de violation. Le Commissariat a aussi pour rôle de sensibiliser la population aux enjeux concernant la protection de

la vie privée et de les lui faire comprendre. En 2013, le ministère de la justice du Canada a proposé le projet de loi C-13 qui vise à criminaliser la distribution d'images personnelles sans le consentement de la personne concernée. En janvier 2014, Ottawa a lancé une campagne intitulée *« Non à la cyberintimidation* ». *« Cette campagne a pour but d'informer les canadiens des répercussions sociales et légales de ce phénomène, de plus en plus répandu chez les jeunes*. », a déclaré le ministre fédéral de la Justice de Canada, Peter Mackay.

En Europe, il existe la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (2002/58). Cette directive vise à protéger de façon spécifique la vie privée sur Internet et elle couvre les aspects laissés de côté par la directive de 1995 sur la protection des données personnelles. En 2012, la commission européenne a proposé un nouveau règlement portant sur un ensemble de règles unique pour toutes les données collectées en ligne afin de garantir qu'elles soient conservées de manière sûre et de fournir aux entreprises un cadre clair sur la façon de les traiter. Cependant, après les révélations faites dans l'affaire d'Edward Snowden, la commission des libertés civiles, de la justice et des affaires intérieurs a procédé, le 21 octobre 2013,à la réforme des règles sur la protection des données, renforçant les droits des citoyens sur celles-ci et augmentant les sanctions. De même, le 28 janvier 2014, l'Association Européenne pour la Défense des Droits de l'Homme (AEDH)[15] a appelé les citoyens, les organisations de la société civile et les parlementaires à être vigilants et à se mobiliser pour demander la révision des textes et des lois afin de suivre le rythme des changements technologiques. Une accélération du processus législatif et une réaction politique sont nécessaires pour offrir le maximum de protection.

Une étude réalisée dans certains pays d'Asie (Bangladesh, Inde, Malaisie, Pakistan, Philippines et Thaïlande) montre que les règles et les lois de protection de la vie privée mises en place visent en général à répondre aux exigences des États-Unis ou de l'Union Européenne dans le but de favoriser les activités commerciales (Tremblay, 2009). Donc, dans la réalité, ces lois ne sont pas dédiées à la protection de citoyens asiatiques. Malgré les directives et les lois implantées dans certains pays, au niveau mondial, il n'existe pas un cadre juridique clair qui couvre la protection de la vie privée sur internet et notamment sur les réseaux sociaux.

Aux États Unis il n'existe pas de loi fédérale sur la protection de la vie privée. Les lois dépendent de chaque état et visent à protéger les mineurs. En Californie la loi baptisée «*loi-gomme*» et promulguée par le gouverneur de Californie Jerry Brown va permettre à partir du 1er janvier 2015 aux adolescents de faire disparaître de leurs pages personnelles sur les réseaux sociaux les photos ou commentaires embarrassants. «*Les erreurs de jeunesse suivent leurs auteurs toute leur vie et leurs empreintes numériques les suivent où qu'ils aillent*» déclare James

15.http://www.aedh.eu/plugins/fckeditor/userfiles/file/Protection%20des%20donn%C3%A9es%20personnelles/CP%20Journ%C3%A9e%20Protection%20des%20donn%C3%A9es.pdf (Vu le 02/02/14).

Steyer fondateur de l'ONG Common Sense Media favorable à la loi dans les colonnes du San Francisco Chronicle[16].

5.5. Solution technique pour la protection de l'information : droit à l'oubli

Pour un être humain, le fait de mémoriser des informations demande souvent un grand effort, alors que l'oubli est un phénomène naturel qui intervient toujours avec le temps (Bouget *et al*, 2013). En revanche, un ordinateur est conçu pour stocker et traiter de l'information. Le fait d'avoir une machine qui oublie est un inconvénient technique majeur en termes d'efficacité et d'intelligence. En plus, il est déjà très difficile de faire disparaître une information de manière efficace si elle a été stockée sur un disque dur (Bouget *et al*, 2013). Même dans la pratique, la suppression d'un fichier consiste généralement à l'effacement d'une entrée dans une table d'indexage (Bouget, 2013). Il ne s'agit donc pas d'un écrasement réel de la donnée elle-même. Le fait d'effacer les informations concernant un utilisateur nous ramène à un problème technique au niveau de l'interconnexion des systèmes d'information et de réseaux d'ordinateurs. Comme exemple de risques majeurs, nous pouvons citer l'augmentation de probabilité d'incohérence des bases de données qui sont souvent répliquées et distribuées géographiquement. Jusqu'à présent, il n'existe aucun outil technique qui peut garantir la cohérence de données. Une approche qui peut être utile est par exemple de stoker des données chiffrées et de garantir l'effacement des clés de chiffrement après un certain délai (Bouget, 2013). Les deux systèmes de ce type les plus connus sont *Ephemerizer* (Perlman, 2005) et *Vanish* (Geambasu *et al*., 2009). Le droit à l'oubli a fait l'objet de beaucoup de débats sur les deux côtés de l'Atlantique, l'Union Européenne et les Etats Unis (Bernal, 2014).

Un autre débat concerne les droits des personnes décédées. Comment une plateforme sociale en ligne peut réagir face à la mort d'un utilisateur?
Rubaker et Vertesi (2010) sont les premiers à travailler sur ce sujet. L'influence de ce problème sur l'entreprise est majeure et dépasse les effets personnels. Par exemple lorsqu'un employé meurt, il laisse sur son profil des informations sensibles concernant l'entreprise. Dans ce cas, un intrus peut *facilement agir en son nom pour pénétrer le système informatique d'entreprise* ou dans le but de réaliser des actions commerciales frauduleuses.

5.6. Vers un système tiers de protection de vie privée entre le réseau social d'entreprise et le système d'information

Devant les failles de protection qui existent entre le réseau social et le système d'information de l'entreprise, nous proposons un système tiers de protection de données entre ces deux entités. Notre système joue le rôle de barrière en vérifiant le niveau de risque de données échangées entre le RSE et le SI. Il est utile à la fois aux

16. http://www.ouest-france.fr/californie-une-loi-pour-effacer-son-passe-sur-les-reseaux-sociaux-1397762 (Vu le 09/02/2014).

clients, aux employés et à l'entreprise. Chacun de ces acteurs peut configurer notre système afin de sécuriser le flux de données échangées et stockées. La Figure 4 montre la position de notre système dans l'architecture de système d'information proposée par Laudon et Laudon (2013).

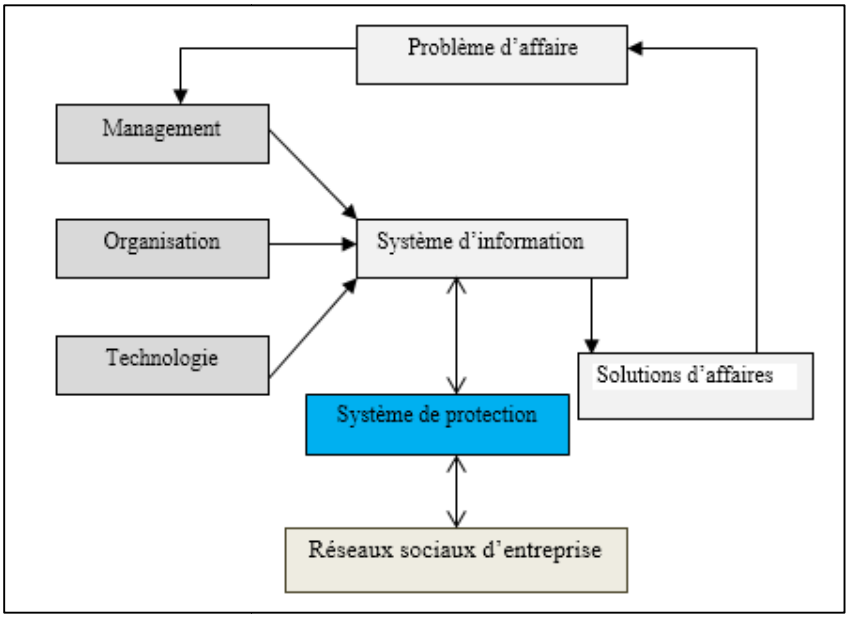

Figure 4. Emplacement de notre système de protection dans l'architecture de Système d'entreprise.

L'architecture générale de *notre système de protection* est constituée de trois modules : le *module de Traitement*, le *module de Classification* et le *module de Décision* (Figure 5).

Le module de traitement assure la préparation et le nettoyage de données, il se compose de deux étapes : *Anonymisation (si nécessaire)* et l'*Étiquetage*. Le module de classification détermine les règles de classification à partir desquelles les données des utilisateurs seront classées (*non risquée, risquée*). Ce module comporte essentiellement deux étapes : analyse de risque et la classification de risque. Il utilise une base contenant des règles applicables aux données provenant des utilisateurs (employés et clients) et des règles applicables aux données provenant du système d'information de l'entreprise. Le module décision se charge de produire le résultat final concernant les données échangées entre le SI et le RSE.

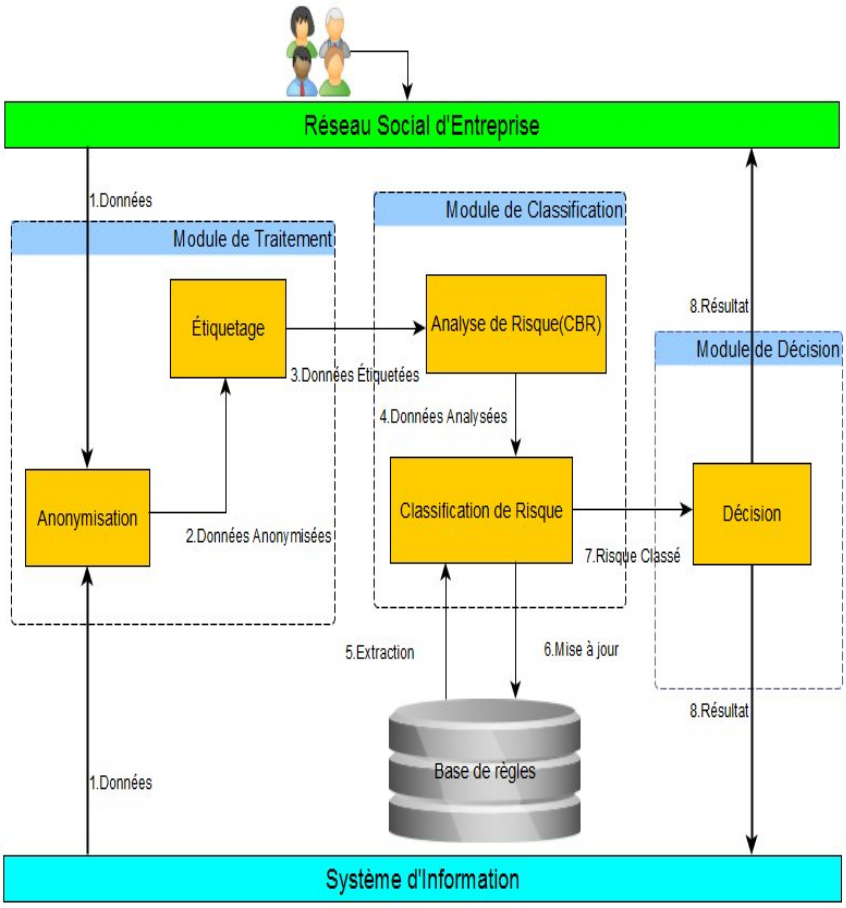

Figure 5. Architecture générale de système de protection.

Dans le système que nous proposons, nous avons deux types de flux de données : le flux provenant du RSE et le flux provenant du SI. Dans les deux cas, l'information est traitée en cinq étapes.

La première étape consiste en *anonymisation* de données. Le but de cette étape est de supprimer toute sorte d'informations permettant d'identifier un employé, un client ou de remonter dans la structure du SI (nom d'utilisateur, numéro, adresse IP…).

La deuxième étape est l'*étiquetage*; elle consiste à extraire les informations sensibles et pertinentes. Il s'agit d'un prétraitement de l'information qui provient du SI et que

l'on veut afficher sur le RSE et vice versa. Ce traitement permet d'étiqueter un certain nombre de mots ou groupe de mots dans le flux d'informations.
La troisième étape se charge de l'*analyse du risque* de données déjà étiquetées, elle est basée sur le *Raisonnement à Base de Cas* (CBR), selon ce principe les données sont analysées en cherchant des cas analogues et en les adaptant au cas considéré. Il s'agit d'une approche de résolution de problèmes qui utilise des expériences passées pour résoudre de nouveaux problèmes (Leake, 1996). Le processus de raisonnement se résume en trois opérations principales : la remémoration, l'adaptation et l'apprentissage. L'étape de remémoration consiste à sélectionner un cas de la base de cas. L'étape d'adaptation a pour but la modification de la solution sélectionnée de façon à construire une solution cible. L'étape d'apprentissage consiste à mettre à jour les connaissances du système à l'issue du raisonnement (Kolodner, 1992). Dans notre système, la structuration initiale de la base de cas peut être construite à l'aide d'un expert ou depuis une base de données. Après la phase d'analyse, les données doivent être catégorisées selon le niveau de risque et de danger et ceci est effectué au niveau de l'étape de *classification* en utilisant une base de règles.

La dernière étape est celle de la *décision*. Elle permet d'avertir si le flux d'information devrait (ou pas) être affiché sur le RSE et/ou stocké dans le SI.
Le système que nous proposons est une nouvelle approche de protection du flux d'information entre le RSE et le SI. L'objectif principal de ce système est de corriger les failles de sécurité créées par l'intégration des réseaux sociaux d'entreprises dans le système d'information.

6. Conclusion

Le réseau social d'entreprise permet d'avoir une meilleure gestion de l'image de l'entreprise. Il permet également de mieux cibler les clients afin de leur présenter les meilleures offres, de mieux informer les personnes qui les suivent et de recruter des employés qui correspondent à leurs critères de sélection. En effet, ils apportent de nombreux avantages à leurs utilisateurs partant de la simple communication d'informations à la possibilité de multiplier et de développer des relations personnelles et professionnelles. Cependant, les réseaux sociaux entrainent des problèmes sérieux. En effet, les facilités apportées par ces réseaux ont mené les utilisateurs, par ignorance ou par indifférence, à divulguer de plus en plus leurs données personnelles.

Grâce aux efforts des éditeurs de réseaux sociaux d'entreprise, mais aussi de logiciels d'affaires dont *SAP*, *Oracle* ou encore *Salesforce*, les possibilités d'interconnecter le réseau social d'entreprise aux applications d'affaires - voire à d'autres briques du système d'information - sont en effet à portée des entreprises. Par exemple, le réseau social Yammer développé par Microsoft est intégré au CRM Microsoft Dynamics et au système de gestion d'informations Microsoft SharePoint ou encore Chatter qui est intégré au CRM Salesforce.com. L'assistant virtuel Shortcuts, développé par Shortways, permet de connecter un réseau social d'entreprise directement aux applications d'affaires, CRM, ERP, etc. Ainsi on obtient la bonne information, au bon moment et selon le contexte désiré.

Cependant, plusieurs menaces à la vie privée ont mené les chercheurs à considérer les risques que posent l'utilisation des réseaux sociaux à la fois sur la vie privée de ses utilisateurs et sur le système d'information de l'entreprise elle-même en déstabilisant son fonctionnement. Ces risques sont d'autant plus significatifs que l'utilisateur ne dispose plus, après divulgation de ses données, de contrôle ni de moyen d'y accéder et éventuellement d'effacer. Néanmoins, tout utilisateur doit être conscient des droits liés aux données collectées et traitées par une entreprise dans les réseaux sociaux. Il s'agit du droit à l'oubli numérique qui garantit pour un utilisateur de limiter la divulgation et la conservation de ses données collectées en retirant son consentement ou en demandant que ses données soient effacées.

Bien que ce droit ait été considéré par la plupart des textes légaux internationaux, il est toujours un sujet de confrontation entre l'entreprise (devoir de mémoire) et l'utilisateur (droit à l'oubli). En effet, les défis techniques que soulève le droit à l'oubli numérique rendent souvent plus facile de conserver les données des utilisateurs que de les effacer surtout que les ressources en mémoire augmentent de manière exponentielle. Ceci dit, plusieurs questions se posent de nos jours quant au sujet de l'application réelle de ce droit à l'oubli notamment dans le contexte des réseaux sociaux.

Face à l'absence d'un cadre législatif clair qui assure la protection de la vie privée et des données mises en jeu dans les réseaux sociaux, les chercheurs sont appelés à la fois à sensibiliser les utilisateurs aux risques potentiels que posent ces réseaux et à développer de nouvelles technologies et outils pour assurer la protection des données.

Bibliographie

Aïmeur E., Brassard G., Rioux J. (2013). Data Privacy : An End User Perspective. *International journal of computer networks and communication*, vol. 6, n° 6, p. 237-250.

Aïmeur E., Gambs S., Ho A. (2010). Towards a privacy-enhanced social networking site, *Proceedings of the 5th International Conference on Availability, Reliability and Security 2010*, Krakow, Poland.

Balagué C., Fayon D. (2010). Quelle est l'utilité des réseaux sociaux pour les entreprises. *Facebook, Twitter et les autres...Intégrer les réseaux sociaux dans une stratégied'entreprise*, Paris, Pearson.

Barnes J. (1954). Class and committees in a Norwegian island parish. *Human Relations*, vol. 7, n° 1, p. 39-58.

Berdnarz A. (2011). 2011 tech priorities: Embrace social media, *Network World*. http://www.networkworld.com/news/2011/010311-outlook-tech-priorities-social-computing.html (Vu le 07/01/2014).

Bernal P. (2014). The EU, the US and Right to be Forgotten. *Reloading Data Protection*, p. 61-77.

Bouget S. (2013). *Implémenter le droit à l'oubli : Dégradation des données par publication Ephémère*. Rapport de stage M2 Recherche, http://dumas.ccsd.cnrs.fr/docs/00/85/49/73/PDF/SimonBouget.pdf (Vu le 15/01/2014).

Bouget S., Gambs S., Pilote G. (2013). Dégradation de données par publication éphémère, *4éme Atelier sur la protection de la vie privée 2013*, les Loges en Josas, France.

Boyd D., Ellison N. B. (2007). Social Network Sites : Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, vol. 13, n° 1, p. 210-230.

Cholet S. (2012). Le réseau social d'entreprise pour communiquer plus efficacement en entreprise. http://www.presse-citron.net/le-reseau-social-dentreprise-pour-communiquer-plus-efficacement-en-entreprise (Vu le 31/01/2014).

Cross R., Parker A., Borgatti S.P. (2000). A bird's-eye view : Using social network analysis to improve knowledge creation and sharing. *Knowledge Directions*, vol. 2, n° 1, p. 48-61.

Deltour F., Plé L., Roussel C.S. (2011). Knowledge sharing in the age of web 2.0 : A social capital perspective. Knowledge Management 2.0 : Organizational Models and Enterprise Strategies. *IGI Publishing*, p. 122-141.

Deswarte Y., Gambs S. (2010). Protection de la vie privée : principes et technologies. *Les technologies de l'information au service des droits : opportunités, défis, limites*, vol. 32.

Dhawan S., Goel S. (2014). Analysis of Pattern of Information Revelation and Site Use Behavior in Social Networking Sites. *International Journal of Computer Applications Technology and Research*, vol. 3, n° 1, p. 42-44.

Dingledine R., Mathewson N., Syverson P. (2003). Reputation in privacy enhancing technologies, *Proceedings of the 12th Annual Conference on Computers, Freedom and Privacy 2003*, San Francisco, USA.

Dorris M.A. (2014). *L'usage des médias sociaux par les relationnistes*. Thèse présentée dans le cadre du programme de maîtrise en communication pour l'obtention du grade maître ès Arts (M.A.), Université d'Ottawa.

Dupont B., Aïmeur E. (2010). Les multiples facettes du vol d'identité. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, vol. 365, n°. 2, p. 177-194.

Fogel J., Nehmad E. (2009). Internet social network communities : Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, vol. 25, n°1, p. 153-160.

Gandouz A. (2012). *PROTECT_U : Un système communautaire pour la protection des usagers de Facebook*. Mémoire de Maitrise en science de l'informatique, Université de Montréal.

Garnier A., Hervier G. (2011a). Le RSE et le SI. *Le réseau social d'entreprise*. Paris, Lavoisier, p. 85-100.

Garnier A., Hervier G. (2011b). Le réseau social d'entreprise. *Le réseau social d'entreprise*. Paris, Lavoisier, p. 59-83

Geambasu R., Kohno T., Levy A., Levy H. Vanish (2009). Increasing data privacy with self-destructing data, *Proceedings of 18th USENIX Security 2009*, Montréal, Canada.

Heitman B. (2012). I totally screwed myself on Facebook. *Hearst Magazines, a Division of the Hearst Corporation, Cosmopolitan*, vol. 252, n° 2.

Herder E., Kawase R. (2012). Considerations for recruiting contributions to anonymised data sets. *International Journal of Technology Enhanced Learning*, vol. 4, n° 1, p. 85-98.

Kin Chan C., Virkki J. (2014). Perspectives for Sharing Personal Information on Online Social Networks. *Social Networking*, vol. 3, n° 1, p. 41-49.

Kobsa A. (2007). Privacy-enhanced web personalization. *The Adaptive Web : Methods and Strategies of Web Personalizatio*n, vol. 4321, p. 628-670.

Kolodner J. L. (1992). An Introduction to Case-Based Reasoning. *Artificial Intelligence Review*, vol .6, p.3-34.

Lafond M., Brosseau P.O., Aïmeur E. (2012). Privacy invasion in business environments, *Tenth Annual International Conference on Security and Trust (PST) 2012*, Paris, France.

Laudon J., Laudon K. (2007). Le SI et les dimensions éthiques et sociales. *Management des systèmes d'information*. Paris, Pearson, p. 141-174.

Laudon J., Laudon K. (2012). Le SI et les dimensions éthiques et sociales. *Management des systèmes d'information.* Paris, Pearson, p. 117-156.

Laudon J., Laudon K. (2013). Information Systems, Organizations, and Strategy. *Management Information Systems*, Toronto, Pearson, p. 60-98.

Lauras H. (2013). *L'impact des réseaux sociaux sur les entreprises a-t-il un rôle essentiel sur leur image*. Mémoire de spécialité Appliquée, France Business School, Paris, France.

Leake D. B. (1996). CBR in Context: The Present and Future. *Case-Based Reasoning: Experiences, Lessons, and Future Directions*, Menlo Park, CA, AAAI Press/MIT Press, p. 2-35.

McKinsey (2012). *The social economy : Unlocking value and productivity through social technologies*. Report McKinsey Global Institute 2012.

Palo Alto Networks (2010). *The Top 10 Social Networking Threats,* http://www.networkworld.com/news/2010/071210-social-network-threats.html (Vu le 15/01/2014).

Parent .S. (2010). *4 P D'une Bonne Gouvernance Des Médias Sociaux,* http://fr.titaninteractif.com/index.php/2010/08/09/4p-bonne-gouvernance-medias-sociaux/ (Vu le 20/01/2014).

Pellerin Clément (2011). *E-réputation & réseaux sociaux : 5 métiers du web 2.0 à (re)découvrir*, http://www.clementpellerin.fr/2011/04/28/e-reputation-reseaux-sociaux-5-metiers-du-web-2-0-a-redecouvrir/ (Vu le 31/01/2014).

Perlman R. (2005). The Ephemerizer : Making data disappear. *Journal of Information System Security*, vol. 1. n° 1, p. 51-68.

Piolle G. (2009). *Agents utilisateurs pour la protection des données personnelles modélisation logique et outils informatiques*. PhD thesis, Université Joseph Fourier - Grenoble I, France.

Rosa C., Garry D. (2001). E-reputation: The role of mission and vision statements in positioning strategy. The Journal of Brand Management, vol. 8, n° 4, p. 315-333.

Rubaker J., Vertesi J. (2010). Death and the Social Network, *Workshop on Death and the Digital 2010*, Atlanta, Georgia, USA.

Smith P.K., Mahdavi J., Carvalho M., Fisher S., Tippett N. (2008). Cyberbullying : its nature and impact in secondary school pupils. *J Child Psychol Psychiatry*, vol. 49, n° 7, p. 376-385.

Stickney R. (2010). *Hospital will fire workers in facebook scandal*, http://www.nbcsandiego.com/news/health/Hospital-Fires-Emps-in-Facebook-Scandal-95794764.html (Vu le 16/01/2014).

Tremblay M. (2009). Flux transfrontières de données et protection de la vie privée : une conjonction difficile, http://www.leppm.enap.ca/leppm/docs/Cahier%20recherche/Cahier%20de%20recherche_Tremblay_Flux%20donn%C3%A9esvf.pdf (Vu le 30/01/2014).

Walter J.P. (2012). *Vingt ans de législation sur la protection des données, rétrospectives et perspectives*,http://www4.ti.ch/fileadmin/CAN/ICPD/PDF/TEMI/Jusletter10373_J_P_Walter_Vingt-ans-PD.pdf (Vu le 15/01/2014).

Wang Y., Kobsa A. (2006). Impacts of privacy laws and regulations on personalized systems, *Proceedings of the Workshop on Privacy-Enhanced Personalization 2006*, Montréal, Canada.

Wicker S.B., Schrader D.E. (2011). PrivacyAware Design Principles for Information Networks. *Proceedings of the IEEE*, vol. 99, n° 2, p. 79-82.

Yang Wang W., Komanduri S., Leon P.,Norcie, G., Acquisti A., Cranor L.F. (2011). I regretted the minute I pressed share : A Qualitative Study of Regrets on Facebook, Symposium on Usable Privacy and Security SOUPS 2011, New York, USA.