# Connectés mais protégés : le pari des réseaux sociaux décentralisés

Francesca Musiani

ParisTech REVIEW:

February 4th, 2011

**Francesca Musiani**
Doctorante et chercheur, Mines ParisTech

# Connectés mais protégés: le pari des réseaux sociaux décentralisés

***L'éclatant succès actuel des réseaux sociaux a un revers: il s'appuie sur le captage, réalisé avec leur consentement mais à des fins marketing, des données personnelles de leurs utilisateurs. Conséquence: les problèmes liés à la protection de la vie privée et des informations personnelles sont aujourd'hui en pleine lumière. Cet article s'intéresse aux développements récents dans le domaine des réseaux sociaux décentralisés, qui permettent de dépasser le dilemme entre préservation de la vie privée et présence sur les réseaux sociaux. Ces outils pourraient même être les premiers à tirer pleinement parti du potentiel social des outils de réseaux virtuels.***

L'idée était pour le moins surprenante : développer un réseau social « open source, contrôlé à l'échelle individuelle, respectueux de la vie privée et multifonction », alors même que le succès massif que connaissent les réseaux sociaux actuels repose sur le bon vouloir des utilisateurs à dévoiler leurs données personnelles, facilitant ainsi une forme sophistiquée de segmentation par « profils ». Plus surprenant encore fut l'intérêt qu'elle éveilla auprès du grand public.

C'est pourtant comme cela que commença l'histoire de Diaspora : à l'été 2010, quatre étudiants de premier cycle de l'Université de New York (NYU) réussirent à lever près de 100 000 dollars – un montant plus de dix fois supérieur à celui qu'ils visaient – pour développer leur idée de réseau social décentralisé. Dan Grippi, l'un des quatre fondateurs, s'en émerveille encore : « Pour quelque mystérieuse raison, tout le monde est tombé d'accord sur ce concept qui tournait autour du respect de la vie privée », explique-t-il dans les pages du New York Times.

Cette raison mystérieuse pourrait bien être la suivante : contre toute apparence, les utilisateurs – ou du moins, certains d'entre eux – sont soucieux de leur vie privée. S'ils apprécient le potentiel des réseaux sociaux en termes d'agrégation, de communication, d'échanges et d'interactions, et souhaitent continuer d'en profiter, les utilisateurs de ces services ne voient pas leur droit à la vie privée comme une monnaie d'échange qu'il leur faudrait céder pour pouvoir accéder à ces réseaux. Ils seraient donc tout à fait prêts à migrer vers une technologie qui leur permette de refuser, au moins partiellement, ce compromis entre respect de l'intimité et accès au réseau; pour lancer le mouvement, ils financent par leurs dons des gens qualifiés qui peuvent ainsi se consacrer au développement de technologies adaptées. En retour, ces derniers – à l'instar des quatre jeunes développeurs de Diaspora, qui sont aujourd'hui les plus présents dans les médias mais sont loin d'être les seuls – assurent que le compromis intimité-connectivité peut être contourné. La solution s'appelle le réseau social décentralisé.

Cet article s'intéresse aux développements en cours dans ce domaine, qui permettront à terme de sortir du dilemme entre protéger sa vie privée et rester connecté, qui se pose sur les réseaux sociaux. Il veut montrer que les outils décentralisés pourraient bien être la première tentative exploitant pleinement les promesses des réseaux virtuels en termes de socialisation, à un moment où le problème de la protection des données et de la vie privée fait la une des médias.

## Décentralisation, réseaux sociaux et protection des données personnelles

Depuis les débuts d'internet, le principe de décentralisation a été à la base de la circulation des transmissions et télécommunications sur le réseau des réseaux. Pourtant, l'introduction du Web en 1990 a progressive-







12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

# Connectés mais protégés: le pari des réseaux sociaux décentralisés

ment conduit à une large diffusion des modèles basés sur l'architecture client-serveur ; les services internet les plus répandus et les plus diffusés (réseaux sociaux, outils de messagerie instantanés, services de stockage de données numériques…) sont conçus à partir de modèles économiques et techniques dans lesquels l'utilisateur final demande une information, une donnée ou un service à de puissants centres de serveurs, qui stockent l'information et gèrent le trafic sur le réseau. Ainsi, même si sur internet le trafic fonctionne sur le principe de la distribution généralisée, il est aujourd'hui concentré autour de serveurs qui délivrent l'accès au contenu. Les observateurs pensent que cette tendance va se développer encore davantage avec la diffusion du modèle de cloud computing dans les marchés où services et plates-formes sont fournis clés en main ; dans ce modèle, le vendeur fournit l'infrastructure physique et le produit logiciel, abritant ainsi à la fois les applications et les données dans un lieu inconnu de l'utilisateur (le fameux « nuage », *cloud* en anglais), et interagit avec ce dernier grâce à une interface client. Ce choix d'organisation des structures et des services, à l'intérieur et en périphérie du réseau, n'est cependant pas le seul possible – et s'il est le plus répandu, il n'est probablement pas le plus efficace. Comme l'ont souligné des chercheurs comme Barbara Van Schewick, Eben Moglen et Niva Elkin Koren – pour n'en citer que trois –, l'une des alternatives possibles, et potentiellement la plus prometteuse, est la décentralisation : concevoir le réseau de manière à ce que les communications et les échanges aient lieu entre des nœuds jouant tous un rôle symétrique dans le système, éliminant ainsi la dualité entre le fournisseur de service et l'utilisateur, typique du modèle serveur/client, et la remplaçant par une situation où chaque client devient serveur.

Les plus célèbres (ou les plus sulfureux, selon les points de vue) modèles de réseaux informatiques décentralisés sont ceux qui sont utilisés, depuis quinze ans, dans les systèmes de partage de fichiers basés sur le *peer-to-peer* (P2P). La technologie *peer-to-peer*, très souvent présentée comme une menace pour les industries où le contenu numérique a une place prépondérante – son utilisation la plus répandue parmi le grand public étant le partage non autorisé de contenus protégés par le droit d'auteur – est, il est vrai, très pratique pour fournir un accès immédiat et gratuit à des copies à la qualité irréprochable ; mais avec une perspective plus large, l'architecture des systèmes P2P est aussi à même d'apporter davantage d'efficacité, de liberté et de stabilité à la distribution de contenu en ligne, grâce aux connections directes entre les utilisateurs devenus des nœuds du système. Facebook et Twitter en tête, ces dernières années ont aussi été celles du succès massif des réseaux sociaux, ces services en ligne permettant à leurs utilisateurs de se construire un profil public ou semi-public au sein d'un réseau, de définir une liste d'utilisateurs avec lesquels ils souhaitent interagir et établir des liens, et de voir la liste des connections qu'eux et leurs amis établissent à l'intérieur du réseau. Parmi les points les plus controversés des réseaux sociaux se trouvent les utilisations que font leurs administrateurs des données personnelles et privées des utilisateurs, donnant souvent à des applications externes la permission d'y accéder, suivant parfois une véritable stratégie commerciale. Relativement peu d'utilisateurs sont aujourd'hui conscients qu'en utilisant de telles applications, ils laissent la possibilité à des publics peu ou pas du tout identifiés d'accéder aux informations d'ordre privé stockées sur les serveurs des entreprises qui fournissent le service – un comportement qualifié récemment de « à risque »par des experts légaux et techniques.

## Vers des réseaux sociaux décentralisés

Récemment, plusieurs projets de recherches et applications commerciales ont tenté, dans ce contexte, de proposer une alternative, en offrant des solutions permettant de contourner au moins certaines de ces limites ; comme l'a résumé Niva Elkin-Koren, des solutions qui préfèreraient « éliminer les intermédiaires » dans les activités de partage et de réseau en ligne. Ces propositions relèvent pour la plupart d'alternatives décentralisées aux services et aux outils qui occupent aujourd'hui une place importante dans notre vie quotidienne sous les noms de Google, Facebook, ou encore







*12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19*

# Connectés mais protégés: le pari des réseaux sociaux décentralisés

Picasa. Et si le modèle du réseau décentralisé était appliqué pour les réseaux sociaux du futur? Les « premiers pas » des réseaux décentralisés marquent-ils l'arrivée de nouveaux paradigmes, de nouvelles possibilités de préserver le droit à la vie privée tout en maintenant, voire en améliorant, l'accès au réseau? Penchons nous sur quelques exemple pour illustrer les développements en cours dans ce secteur, autour du très médiatique cas Diaspora et au-delà.

Le projet de développement de réseaux privés virtuels (Virtual Private Networks, VPNs) «sociaux» , en cours à l'Université de Floride cherche à relier les utilisateurs sur un réseau virtuel, dans lequel des liens de type *peer-to-peer* sont automatiquement générés au niveau de la couche application (la couche du réseau qui fournit les services nécessaires au bon fonctionnement de l'application, s'assurant qu'elle peut communiquer avec un autre programme d'application sur le réseau sans encombre), selon les liens établis au niveau de l'infrastructure du réseau social. Dans ce système, chaque utilisateur fait office d'autorité de certification pour la couche correspondant à son profil, donnant à chaque membre de sa «couche» (autrement dit ses contacts) un certificat ou une clé qu'il a lui-même généré.

NoseRub, au nom évocateur (en anglais, l'équivalent d'un «caillou dans la chaussure»), est un protocole de réseau social décentralisé pour lequel un prototype existe déjà, et qui autorise les applications utilisant ce même protocole à stocker des informations sur les données composant le profil de chaque contact. Ceci permet aux utilisateurs du réseau de garder les informations de leur profil sur leurs propres terminaux, et à leurs terminaux d'interagir et de se synchroniser automatiquement.

Appleseed, un projet de réseau social décentralisé, est parti de la volonté de considérer l'utilisateur comme un « citoyen du net plutôt qu'un consommateur à cibler» et d'une «attention particulière accordée à la vie privée et à la sécurité», perçues comme constamment foulées au pied par la publicité, le placement de produit et l'échange de données largement présents dans les réseaux sociaux «classiques». Après une période difficile sur le plan financier, le projet est de nouveau sur les rails et vise à construire un modèle de réseau distribué, sur lequel le profil d'un site Appleseed est capable de se lier avec un profil sur un autre site Appleseed, permettant ainsi une interaction directe entre les deux.

Plus récemment, le projet de réseau social distribué Diaspora a levé, comme évoqué dans l'introduction, près de dix fois plus de fonds que ne s'y attendaient initialement ses créateurs, quatre étudiants en programmation de NYU. Pour protéger les données privées de ses utilisateurs, le concept de Diaspora est de faire de ces derniers les hôtes du nœud qui contient leurs informations personnelles : comme l'a souligné le professeur de droit Eben Moglen, mentor du projet (devenu depuis conseiller informel), cela représente « la seconde génération d'architecture de réseau social, qui met le partage à la portée de tous, sans intermédiaire qui centralise toutes les données pour tout le monde ». L'idée sous-jacente, comme celle qui prévaut pour ses prédécesseurs, est que l'entreprise renonce partiellement ou totalement à accéder aux données personnelles de ses utilisateurs, garantissant ainsi leur protection – augmentant par la même occasion le contrôle exercé par les utilisateurs, mais aussi leurs responsabilités, vis-à-vis de leurs informations personnelles. Des ordinateurs totalement indépendants, que les développeurs de Diaspora nomment des «graines», sont amenés à se connecter directement entre eux. Un internaute a comparé les graines de Diaspora à des agrégateurs « qui rassemblent le contenu qui vous concerne sur internet dans un lieu central, votre serveur. Reliez votre graine à la mienne et nous pouvons partager et échanger. (...) En bref, vous abritez votre propre profil, qui est une agrégation de votre vie en ligne, et vous le partagez avec un groupe de gens sélectionné ».

Le plus grande inconnue pour ces projets de réseaux sociaux décentralisés est sans doute de savoir si les utilisateurs eux-mêmes seront prêts non seulement à migrer vers une autre plate-forme, mais aussi vers une application dont la prise en main et les bénéfices







*12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19*

# Connectés mais protégés: le pari des réseaux sociaux décentralisés

d'utilisation sont peut-être moins immédiats. La valeur ajoutée offerte par ces projets étant en résumé la possibilité pour les utilisateurs de générer leur propre petit serveur abritant les données de leur profil, ces produits risquent, selon certains, de ne pas toucher suffisamment d'adeptes parmi des utilisateurs habitués à une interface moins compliquée, accessible au plus grand nombre. Pourtant, comme le note un commentateur, « qu'un groupe de développeurs ait lancé une levée de fonds pour créer une alternative à Facebook – et que des personnes aient répondu à l'appel – représente peut-être la critique la plus accablante envers ce réseau social ». Si l'ingrédient manquant est la notoriété et un large soutien, le moment est peut-être idéal pour se lancer et accélérer les choses.

**Une opportunité sociale**

Les différents projets et applications qui travaillent sur la décentralisation appliquée aux réseaux sociaux représentent peut-être la première réelle tentative d'optimisation des outils de mise en réseau en termes de sociabilité. Comme l'ont remarqué les chercheurs de l'Université de Floride, un nombre important d'internautes interagissent systématiquement avec des réseaux sociaux en ligne ; pourtant, si les infrastructures des réseaux sociaux sont tout à fait adéquates et orientées pour mettre à jour et établir des liens entre les personnes, elles sont très mal adaptées quand il s'agit de permettre à un utilisateur d'établir des liens avec ses pairs sous la forme d'un réseau. Le défi, en même temps que la clé pour des réseaux sociaux plus robustes et plus sûrs, est donc d'envisager des architectures innovantes capables d'intégrer les outils de réseau au niveau de l'interface ET de l'application, améliorant ainsi d'un même coup la connectivité et la protection de la vie privée.

La protection des données privées des utilisateurs de réseaux sociaux devrait, selon toute probabilité, s'améliorer par deux moyens. D'un côté, l'utilisation d'architectures décentralisées, distribuées ou de *peer-to-peer* appelle à une remise à plat des pratiques de gestion de données, en prenant en compte les réseaux sociaux les plus utilisés aujourd'hui ; cette reconfiguration implique des évolutions profondes dans le statut de fournisseur de service, dans la nature des informations auxquelles il a accès, et dans les lieux physiques où sont effectués les opérations de stockage et de partage des contenus générés par l'utilisateur. D'un autre côté, ces applications progressent aussi vers l'élaboration de solutions à certaines faiblesses des réseaux de *peer-to-peer* « classiques », en renforçant le caractère personnel des requêtes et des processus d'autorisation liées à l'établissements de liens sur le réseau, qui sont mises en œuvre pour les commandes de type « Ajouter comme ami » ou l'attribution de différents degrés de confiance à différents contacts pris au sein du réseau.

Dans son discours prononcé à 2010 à NYU et cité par l'équipe de Diaspora comme leur première et principale source d'inspiration, Eben Moglen affirmait que, dans un paysage de services internet dominé par le paradigme client-serveur, ce qui est actuellement rangé sous l'étiquette de la tendance *cloud computing* n'est rien d'autre que « des serveurs qui ont gagné [davantage de] liberté. Liberté de bouger. Liberté de louvoyer ; de combiner et de diviser, de ré-agréger et d'utiliser toute sorte d'astuces. Les serveurs ont gagné en liberté. Les clients n'ont rien gagné ». Pourtant, un gain pour les clients ne signerait pas forcément la mort du *cloud computing*, et réciproquement. Dans un réseau distribué, où la frontière entre client et serveur devient plus floue ou tout à fait inexistante, cette liberté serait aussi distribuée, tout comme le « nuage ». En fait, le nuage décentralisé, à l'image de la plate-forme de service intégrée française TioLive LLC et de son service d'interface et d'hébergement TioLive Grid, serait conçu pour répartir la puissance de calcul et les ressources du nuage entre les terminaux de tous les utilisateurs-contributeurs –une fois encore, avec l'idée que « liberté totale de l'utilisateur au sein du 'nuage' et possibilité pour lui de contrôler entièrement, et par ses propres moyens, ses données personnelles » ne sont pas incompatibles.

Des profils hébergés chez l'utilisateur, moins d'intermédiaires, des « nuages » constitués d'utilisateurs... Il y a beaucoup à faire pour rééquilibrer la balance, et le







12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

# Connectés mais protégés: le pari des réseaux sociaux décentralisés

fait que les gens en soient de plus en plus conscients – pas seulement quelques développeurs, mais aussi de nombreux utilisateurs – est probablement la raison « mystérieuse » pour laquelle, comme le remarquait il y a quelques mois Dan Grippi « tout le monde est tombé d'accord sur ce concept qui tournait autour du respect de la vie privée ». La balle est maintenant dans le camp des chercheurs, des entreprises et des communautés d'utilisateurs pour exploiter pleinement les opportunités liées à la décentralisation et aller ainsi vers un monde mieux connecté où – bien que constamment transformée et recomposée – la sphère privée peut exister et être respectée.

Academic


- Biddle, P., P. England, M. Peinado, & B. Willman (2002). The Darknet and the Future of Content Distribution [Le réseau de partage privé et l'avenir de la distribution de contenu]. ACM Workshop on Digital Rights Management.
- Boyd, D. & N. Ellison (2007). Social Network Sites: Definition, History, and Scholarship [Le sites de réseaux sociaux : définition, historique et travaux académiques]. Journal of Computer-Mediated Communication, 13 (1).
- Diffie, W., & S. Landau (2007). Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition [La vie privée en ligne de mire : les pratiques d'écoute et de chiffrement, édition revue et mise à jour]. Cambridge, MA: The MIT Press.
- Elkin-Koren, N. (2006). Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic [Rendre la technologie plus visible : la responsabilité des fournisseurs de services internets dans le trafic peer-to-peer]. New York Journal of Legislation and Public Policy, 9.
- Figueiredo, R. J., P. O. Boykin, P. St. Juste, & D. Wolinsky (2008). Social VPNs: Integrating Overlay and Social Networks for Seamless P2P Networking [Les réseaux sociaux privés virtuels : combiner les technologies de recouvrement et des réseaux sociaux pour des réseaux peer-to-peer d'un nouveau genre]. Compte-rendu des 17ème rencontre "Enabling technologie" de l'IEEE, 2008, Washington, DC: IEEE Computer Society.
- Gross, R. & A. Acquisti (2005). Information Revelation and Privacy in Online Social Networks [La mise au jour des informations et la vie privée dans les réseaux sociaux en ligne], Compte-rendu du colloque « Vie privée dans la société numérique » de l'ACM, 2005, Alexandria, VA, USA. New York, NY: ACM.
- Le Fessant, F. (2009). Les réseaux sociaux au secours des réseaux 'pair-à-pair'. Défense nationale et sécurité collective, 3.
- Moglen, E. (2010). Freedom In The Cloud : Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing [La liberté dans les nuages : liberté de code, vie privée et sécurité pour le web 2.0 et le cloud computing]. Rencontres ISOC, bureau de New York, 5 février 2010.
- Solove, D. (2006). The Digital Person: Technology and Privacy in the Information Age [L'être numérique : technologie et vie privée à l'âge du tout-information]. New York, NY: NYU Press.
- Van Schewick, B. (2010). Internet Architecture and Innovation [Architecture d'internet et innovation], Cambridge, MA: MIT Press.
- Wood, J. A. (2010). The Darknet: A Digital Copyright Revolution [Les réseaux de partage privés : la révolution numérique du droit d'auteur], Richmond Journal of Law & Technology, 16 (14).








12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19