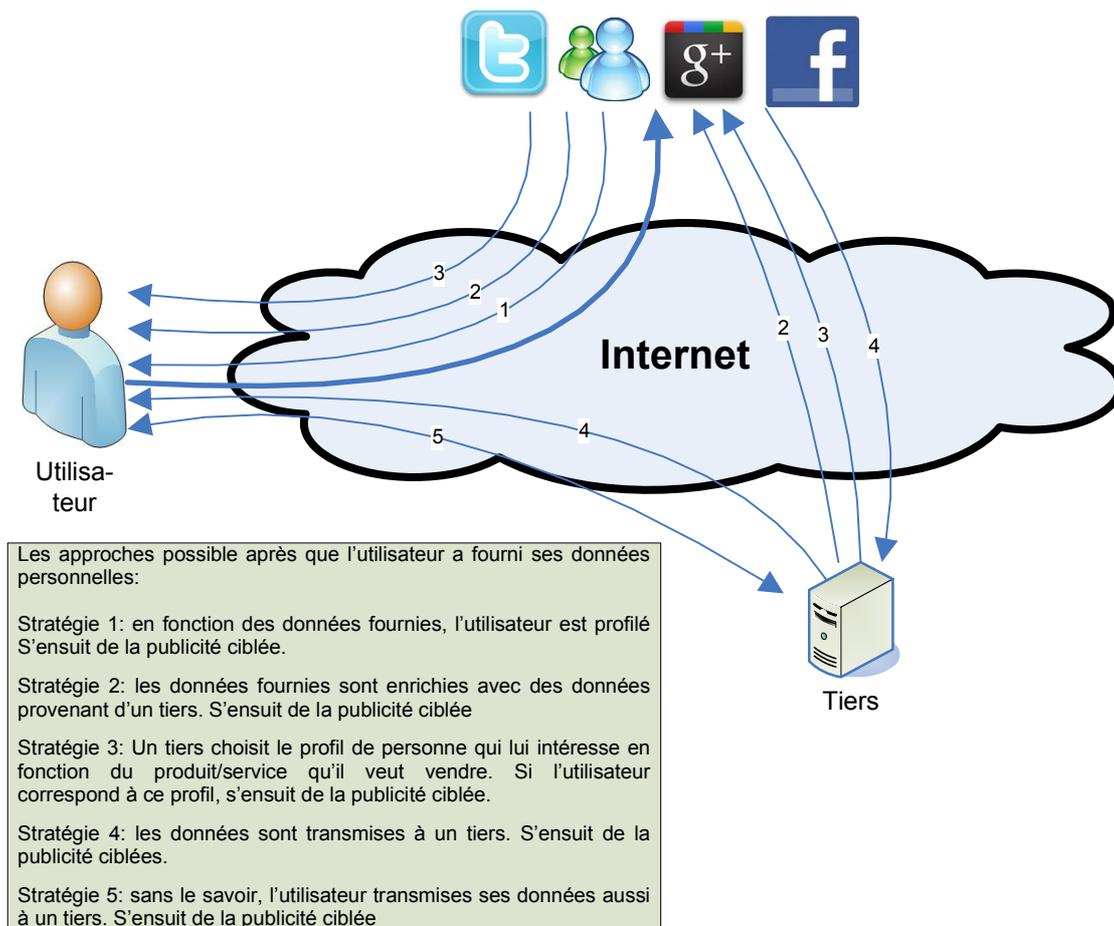


Données personnelles sur Internet: quo vadis?

Un nombre croissant de personnes publie toujours plus d'informations personnelles sur Internet (blog, chat, réseau social, forum de discussion, etc.). Ces informations touchent tous les aspects de la vie privée, des plus futiles jusqu'aux plus délicats comme des opinions religieuses ou de graves maladies¹. Au-delà des raisons qui poussent à ces comportements², il est plus intéressant de comprendre ce qui arrive à ces informations du point de vue de la protection des données. Qui peut y accéder? Dans quels buts seront-elles utilisées? Est-il possible de les effacer?

Pour pouvoir répondre à ces questions et en comprendre tous les aspects, il faut examiner les différentes approches utilisées par les différents fournisseurs de services (dans l'illustration suivante les logos ne figurent qu'à titre explicatif):



¹ Voir <http://www4.ti.ch/can/icpd/convegno/home/video-e-documentazione/>, contribution „Tavola Rotonda“, orateur B. Baeriswyl, Président de privatim, à partir de la minute 4:15 (en allemand)

² Voir <http://www4.ti.ch/can/icpd/convegno/home/video-e-documentazione/>, contribution „Tavola Rotonda“, orateur F. Pizzetti, Président du Garante italiano della protezione dei dati, à partir de la minute 13:15 (en italien)

Comme on vient de le voir dans l'illustration précédente, il est illusoire de penser qu'en transmettant des informations à une plateforme informatique, elles ne restent que dans la plateforme en question. La réalité, qui ressort souvent des conditions d'utilisation que l'utilisateur accepte (généralement sans les avoir lues), est bien différente: les stratégies permettant de profiter au mieux des informations obtenues sont en fait nombreuses:

- **Stratégie 1:** il s'agit de publicité directe. Typiquement, on participe à un concours online (en fournissant son nom, prénom, adresse et email) et ces informations sont ensuite utilisées à des fins publicitaires. Des solutions plus sophistiquées, très souvent utilisées par les cartes de fidélité des grands magasins, prévoient en outre un profilage en fonction des marchandises achetées et des données d'identité (exemple: il est fort probable qu'une publicité pour des couches ne puisse pas intéresser un jeune homme de 16 ans, tandis que le même produit peut intéresser une femme de 25 ans qui vient d'acheter des vêtements pour un bébé de 6 mois). Cela peut conduire à une publicité plus ciblée, en fonction des intérêts présumés de l'utilisateur.
- **Stratégie 2:** même chose que le cas précédent, mais les données sont enrichies avec des données provenant d'un tiers, par exemple avec les conditions économiques de l'utilisateur (exemple: pour celui qui vend un produit de luxe, il peut être très important de connaître les conditions économiques des personnes).
- **Stratégie 3:** l'entreprise tierce, en fonction du produit/service qu'elle offre, définit son profil-cible de personnes et le communique à une plateforme informatique à laquelle l'utilisateur avait transmis ses données personnelles. Si les profils correspondent, l'utilisateur recevra ensuite la publicité de l'entreprise tierce (typique sur Facebook, par exemple pour une entreprise qui offre un service de rencontre en Romandie: il est fort probable que ce service intéresse plus un homme célibataire de 35 ans résidant à Lausanne plutôt qu'une femme mariée de 22 ans résidant à Berlin).
- **Stratégie 4:** les données transmises par l'utilisateur à une plateforme informatique sont vendues à un tiers qui pourra les utiliser à d'autres fins, par exemple pour envoyer de la publicité, mais aussi pour revendre les données à une autre plateforme informatique qui pourra ainsi enrichir ses informations sur l'utilisateur (stratégie 2).
- **Stratégie 5:** souvent en visitant un site Internet, en réalité on communique sans le savoir avec (beaucoup) d'autres sites Internet. Les portails d'information en ligne qui donnent la possibilité de commenter un article en utilisant un réseau social constituent un exemple classique. Très souvent, simplement en lisant un article en ligne, l'utilisateur communique aussi avec le réseau social en question, en lui transmettant des informations sur l'article qu'il a lu (et qui donc l'intéresse probablement).

Ces différentes stratégies peuvent bien évidemment être combinées à bien plaisir.

La diffusion de ces phénomènes peut être montrée en utilisant des instruments d'analyse.

1. Analyse quantitative

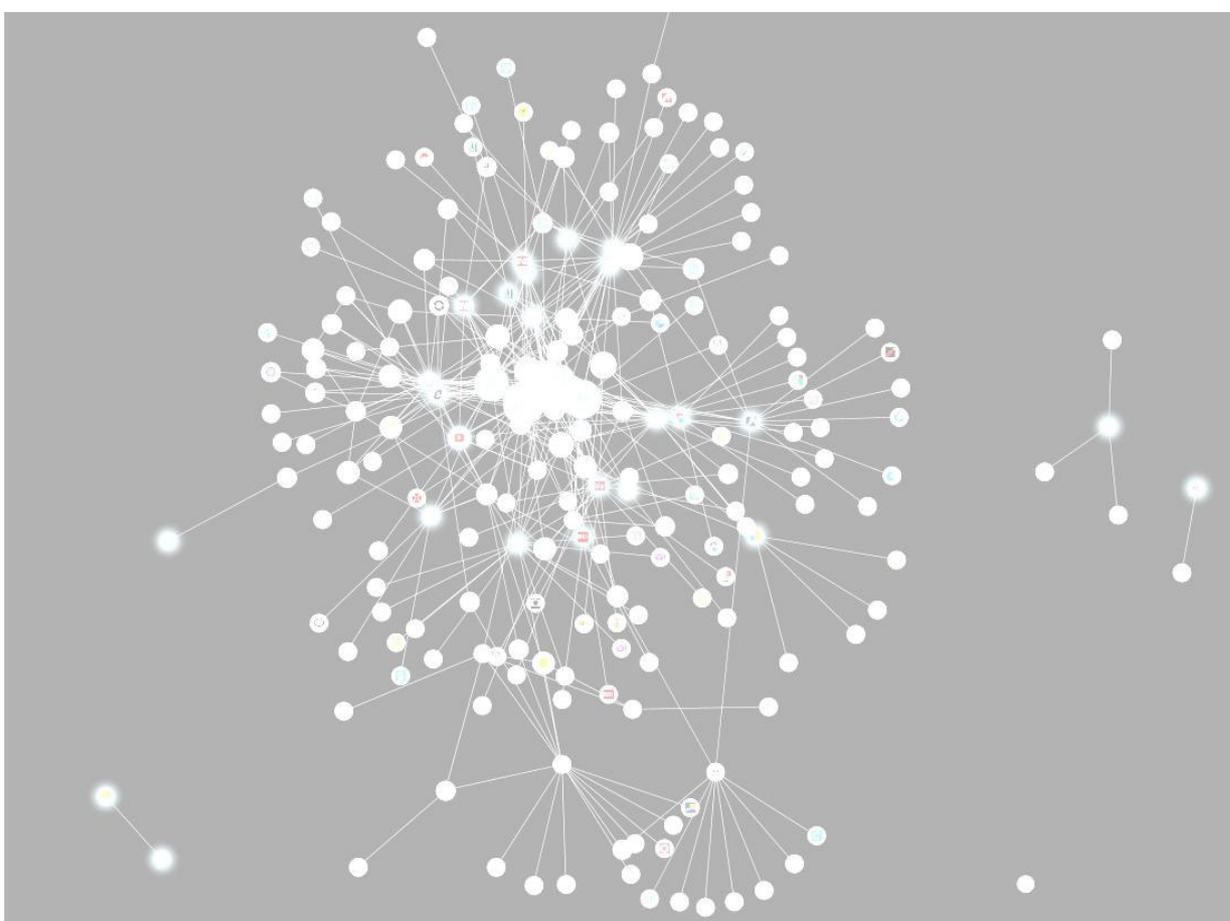
Il existe des instruments appelés debugging proxy³, qui permettent de savoir quelles informations on est en train de transmettre/recevoir sur Internet. Le but original de ces instruments est de trouver des fautes dans la phase de développement software. Les mêmes instruments

³ Par exemple, pour un produit gratuit en essai durant 30 jours voir <http://www.charlesproxy.com/>. Après les 30 jours, le produit continue à fonctionner mais il se bloque après 30 minutes.

peuvent aussi être utilisés pour vérifier la diffusion de la stratégie 5. Il est conseillé d'essayer sur son propre ordinateur ou d'assister à une démonstration⁴.

2. Analyse qualitative

Comme on vient de le voir, les données de l'utilisateur sont transmises à beaucoup de sites tiers. De plus, ces sites ne reçoivent pas seulement des données à partir d'une seule plateforme informatique. En fait, un site tiers peut recevoir des informations en provenance de dizaines de sites différents, ce qui permet ainsi de mieux profiler l'utilisateur. Ce phénomène peut être montré en utilisant des instruments informatiques particuliers⁵. À nouveau, il est conseillé d'essayer de les installer et de vérifier la situation. Le résultat comprend une représentation graphique montrant quel site a transmis des données à quel autre site. Après quelques jours de navigation normale sur Internet, la situation pourra être la suivante⁶:



Les cercles représentent les différents sites Internet, tandis que les lignes qui les relient montrent les communications entre les différents sites. La diffusion de la stratégie 4 est ainsi évidente.

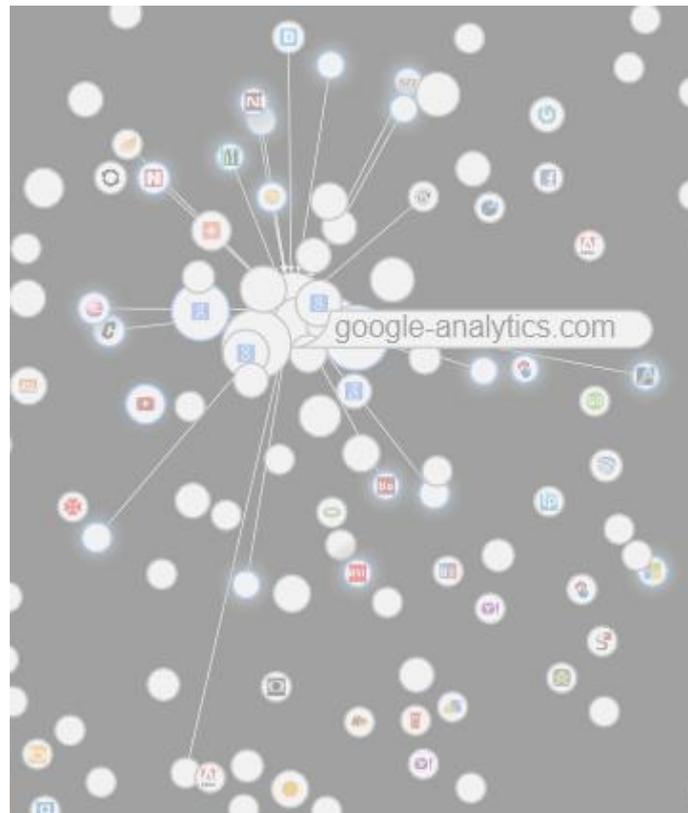
⁴ Voir <http://www.rsi.ch/linearossa/index.cfm?scheda=20930>, à partir de la minute 33:15 (en italien).

⁵ Par exemple l'Add-On pour Firefox appelé Collusion, téléchargeable gratuitement (<https://addons.mozilla.org/it/firefox/addon/collusion/>).

⁶ Les couleurs dans cette image ainsi que dans la suivante ont été modifiées pour améliorer la visibilité et faciliter l'impression

À noter que, en réalité, la plupart de ces sites n'ont jamais été directement visités. Ils ont uniquement reçu/transmis des informations.

En sélectionnant un cercle on pourra en outre savoir quel site il représente et avec quels autres sites il a communiqué. À nouveau, en prenant comme exemple un site jamais directement visité, on montre la diffusion du phénomène.



Les informations fournies par les utilisateurs ont une très grande valeur commerciale: elles sont le prix payé par l'utilisateur pour bénéficier d'un service en apparence gratuit.

Des trois questions posées au début de cette contribution, il reste à clarifier la dernière: «après avoir publié des informations sur Internet, est-il possible de les effacer?». Malheureusement, la réponse ne peut être que négative: tout ce qui est publié sur Internet devient potentiellement accessible à tout le monde et pour toujours.

Conclusion

Les réseaux sociaux sont des instruments qui, comme tous les instruments, peuvent être bien ou mal utilisés. Par exemple, Facebook vient de donner la possibilité de se déclarer «donneur d'organes» (nous ne nous n'exprimerons pas sur la validité légale d'une telle déclaration par le biais de Facebook). Dans un pays qui souffre d'une carence chronique de donateurs, cela peut bien sûr avoir des effets positifs. Comme on l'a vu, il y a aussi des aspects négatifs, liés en particulier aux atteintes à la sphère privée.

Chaque citoyen doit être libre de choisir comment utiliser ces instruments, mais pour pouvoir choisir en toute connaissance de cause, il doit aussi être informé et savoir quelles sont les conséquences.