Réseaux sociaux et confidentialité

Quand nous concluons un contrat avec un fournisseur de services de l'Internet, nous cliquons généralement *Oui* sur la case « Acceptez-vous les termes de la license ? » sans les lire. Pourtant, il vaudrait mieux les lire car ces contrats accordent fréquemment au fournisseur des droits considérables et le seul fait de cocher la case signifie que nous acceptons de les lui donner.

La légalité de certaines dispositions des licences est sujette à caution, mais l'Internet est international et complexe, et la jurisprudence encore minimale. Qui serait prêt à dépenser beaucoup d'argent pour engager des poursuites aux États-Unis contre une multinationale, en étant prêt à y consacrer des années, et pour un résultat final aléatoire ?

L'exemple de Google

Le fait que beaucoup de fournisseurs de services de l'Internet sont basés aux États-Unis est problématique car la loi américaine accorde peu d'importance à la protection de la vie privée. Aux États-Unis, on peut consentir à la perte de droits d'une manière qu'un juge européen regarderait avec suspicion.

Les *Conditions d'utilisation de Google* sont un exemple. Voici quelques extraits [1] :

> Nous pouvons être amenés à vérifier les contenus pour s'assurer de leur conformité à la loi ou à nos conditions d'utilisation. [...]
>
> En soumettant des contenus à nos Services, par importation ou par tout autre moyen, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage ou de distribution public desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services.

Si vous êtes chez Google, vous avez donc accepté que tout ce que vous y mettez peut — dans les limites de la loi — être utilisé ou publié n'importe où dans le monde si cela concerne l'exploitation ou la promotion de Google.

---

[1] Source : http://www.google.com/policies/terms, 29 février 2013.

Voici quelque extraits des *Règles de confidentialité* [2] :

> Lorsque vous utilisez nos services ou que vous affichez des contenus fournis par Google, nous pouvons automatiquement collecter et stocker des informations dans les fichiers journaux de nos serveurs. Cela peut inclure :
>
> - la façon dont vous avez utilisé le service concerné, telles que vos requêtes de recherche.
> - des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des SMS et les types d'appels.
> - votre adresse IP.
> - des données relatives aux événements liés à l'appareil que vous utilisez, tels que plantages, activité du système, paramètres du matériel, type et langue de votre navigateur, date et heure de la requête et URL de provenance.
> - des cookies permettant d'identifier votre navigateur ou votre Compte Google de façon unique.
>
> [...] Nous pouvons également être amenés à utiliser différentes technologies permettant de vous localiser, telles que les données du capteur de votre appareil permettant par exemple d'identifier les points d'accès Wi-Fi et les antennes-relais se trouvant à proximité. [...]
>
> Nous pouvons être amenés à collecter et à stocker des données (y compris des données personnelles) sur l'appareil que vous utilisez, à l'aide de mécanismes comme le stockage sur navigateur Web (HTML5) et les caches de données d'application. [...]
>
> Les informations personnelles que vous fournissez pour l'un de nos services sont susceptibles d'être combinées avec celles issues d'autres services Google (y compris des informations personnelles) [...].

Une autre disposition peut paraître innocente :

> Nous demandons toujours votre autorisation avant de communiquer à des tiers des données personnelles sensibles.

Mais cette protection du client concerne les données personnelles *sensibles* (par exemple notre état de santé ou nos opinions politiques). Qu'en est-il des données personnelles qui ne sont pas considérées comme sensibles (nom, adresse, etc.) ? Le texte répond à cette question quelques paragraphes plus bas :

> Nous transmettons des données personnelles à nos filiales ou autres sociétés ou personnes de confiance qui les traitent pour notre compte, selon nos instructions, conformément aux présentes Règles de confidentialité et dans le respect de toute autre mesure appropriée de sécurité et de confidentialité.

---

[2] Source : http://www.google.com/policies/privacy, 29 février 2013.

Google est partout

Même ceux qui ne sont pas chez Google sont chez Google :

1° Chaque fois qu'une personne qui n'est pas cliente de Google envoie un message électronique à un compte Gmail, le message est analysé — cela sans son consentement puisqu'elle n'a pas coché la case « Acceptez-vous les termes de la license ».

Google appelle cela *content extraction* (extraction de contenu). Cette opération permet même une analyse sémantique des messages (*knowledge graph*, profil de connaissance).

Une solution à ce problème consiste à éviter Gmail et prendre un compte chez un fournisseur de services européen (exemple : http://www.laposte.net).

2° Quel que soit le navigateur utilisé, la recherche effectuée par une personne est analysée et ajoutée aux données de son profil chaque fois qu'elle utilise le moteur de recherche de Google.

3° Si cette personne utilise le navigateur Chrome, les adresses des sites auxquels elle accède sont transmises à Google.

4° Si elle se rend sur Youtube, les vidéos qu'elle visionne sont consignées par Google et il en va de même avec ses rendez-vous si elle emploie Google Calendar. Le même problème se pose avec les autres services.

5° Une faille moins connue est Google Translate. Si une personne utilise cet outil pour une traduction, tout est enregistré. Cela veut dire, par exemple, que le fait de traduire un projet de brevet avec Google Translate fournit automatiquement une copie du texte à Google.

Cela veut dire qu'il y a un problème juridique derrière Google Translate : les documents confidentiels ne doivent pas être communiqués à des tiers ; or le seul fait de les traduire avec Google Translate revient à les transmettre à Google.

Greg Conti, de la U.S. Military Academy de West Point, a écrit un livre sur le sujet intitulé *Googling Security* [3]. Il a dénombré plus de cinquante services de Google qui collectent des informations personnelles.

La situation a conduit Microsoft à créer un site dédié à ces pratiques, http://www.scroogled.com [4].

---

[3] Greg CONTI, *Googling Security*, Addison-Wesley, New York, 2008.

[4] Le mot *Scroogled* est une contraction de l'expression *Screwed by Google* (roulé par Google).

La légalité des pratiques de Google

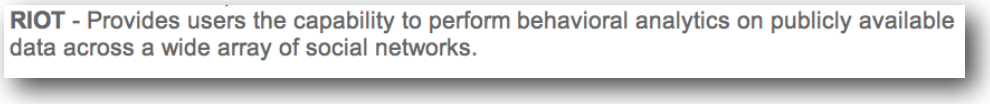
Aux États-Unis, la faiblesse des règles sur la protection de la vie privée a peut-être pour résultat que les pratiques de Google sont légales, mais c'est plus douteux en Europe.

Un Espagnol a récemment découvert que le moteur de recherche de Google permettait de trouver une information personnelle sensible, la vente aux enchères d'un de ses biens en raison du non paiement de ses cotisations de Sécurité sociale. Google ayant refusé de supprimer cette information, l'Agence espagnole de protection des données a porté en 2012 cette affaire devant la Cour de justice de l'Union européenne [5]. Pour autant qu'elle juge la question recevable, la Cour devra notamment se déterminer sur un point qui intéresse beaucoup les juristes : est-ce que Google, entreprise californienne, est soumise au droit espagnol, sachant qu'il existe bien une filiale espagnole, mais que cette filiale se limite à gérer la publicité sur le site [6] ?

D'autre part, la CNIL et les vingt-six autres organismes nationaux de protection de la vie privée de l'Union européenne ont décidé début 2013 d'intenter une action répressive contre l'entreprise parce qu'elles pensent que les pratiques de Google ne sont pas conformes à la législation européenne [7].

L'exemple du logiciel RIOT de Raytheon

Raytheon, l'une des principales entreprises d'armement américaines, a réalisé un logiciel appelé RIOT (*Rapid Information Overlay Technology*), dont le but est de scanner et analyser les informations disponibles sur l'Internet au sujet d'une personne (http://www.raytheon.com/technology_today/2012_i1/eet.html) :



Ce logiciel scanne les mlliards de données présentes sur le web et les réseaux sociaux (LinkedIn, Facebook, Twitter, Picasa, Foursquare, etc.) et réunit l'ensemble des informations qu'il trouve sur

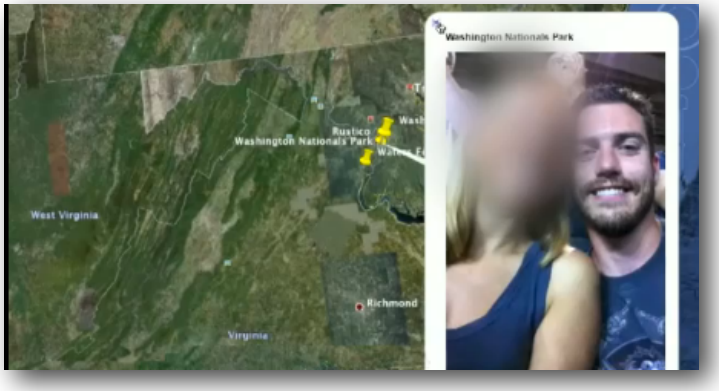
---

[5] Rosario G. GÓMEZ, « El Tribunal de la UE abre el primer proceso sobre privacidad en la Red », *El País*, 26 février 2013.

[6] SEVACH, « Cuestión prejudicial candente : Google ante el Tribunal de Justicia de la Unión Europea », *Contencioso.es*, 11 mai 2012.

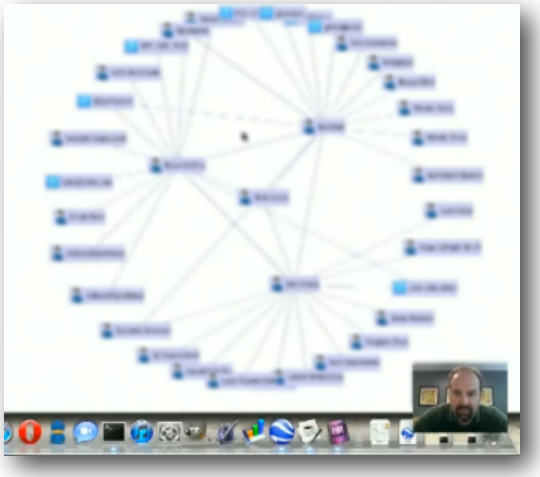
[7] « Vie privée : la CNIL engage une action répressive contre Google », *Le Nouvel Observateur*, 26 février 2013.

une personne, y compris les photos sur lesquelles elle apparaît. Si ces informations n'apparaissent pas dans les commentaires, la date et l'endroit où les images ont été prises sont extraits des données EXIF des photos. L'image ci-dessous montre que RIOT a trouvé une photo de la personne ciblée et a établi qu'elle a visité le parc national de Washington en compagnie d'une autre personne qui apparaît également sur la photo (et qui n'est pas floutée sur l'image affichée à l'origine par le logiciel).



En scannant les données de géolocalisation, RIOT peut reconstituer les déplacements de la personne et afficher les endroits qu'elle fréquente le plus souvent. On peut affficher un graphique qui montre à quels moments de la semaine elle se trouve à un endroit donné.

Le cercle des amis et connaissances de la personne est identifié notamment grâce à la reconnaissance faciale. On peut afficher leurs noms avec les adresses et les numéros de téléphone (image ci-dessous).



On peut voir comment le logiciel s'utilise en visionnant une vidéo confidentielle de Raytheon parvenue au *Guardian* [8], qui l'a mise en ligne à l'adresse http://www.guardian.co.uk/world/video/2013/feb/10/raytheon-software-tracks-online-video (les deux images de cette page sont extraites de cette vidéo).

À première vue, RIOT viole les règles sur la protection de la vie privée, mais les États-Unis ont une législation anti-terroriste qui permet beaucoup de choses.

RIOT n'est pas un cas unique. D'autres applications peuvent susciter des inquiétudes, notamment Perfectcitizen, de la National Security Agency [9].

---

[8] Ryan GALLAGHER, « Software that tracks people on social media created by defence firm », *The Guardian*, 10 février 2013.

[9] « Statement of Work for (U) Perfectcitizen », NSA, Fort Meade, 8 septembre 2009. Documents déclassifiés accessibles sur le site de l'Electronic Privacy Information Center, http://epic.org/foia/nsa/NSA-PerfectCitizen-FOIA_Docs.pdf, décembre 2012.