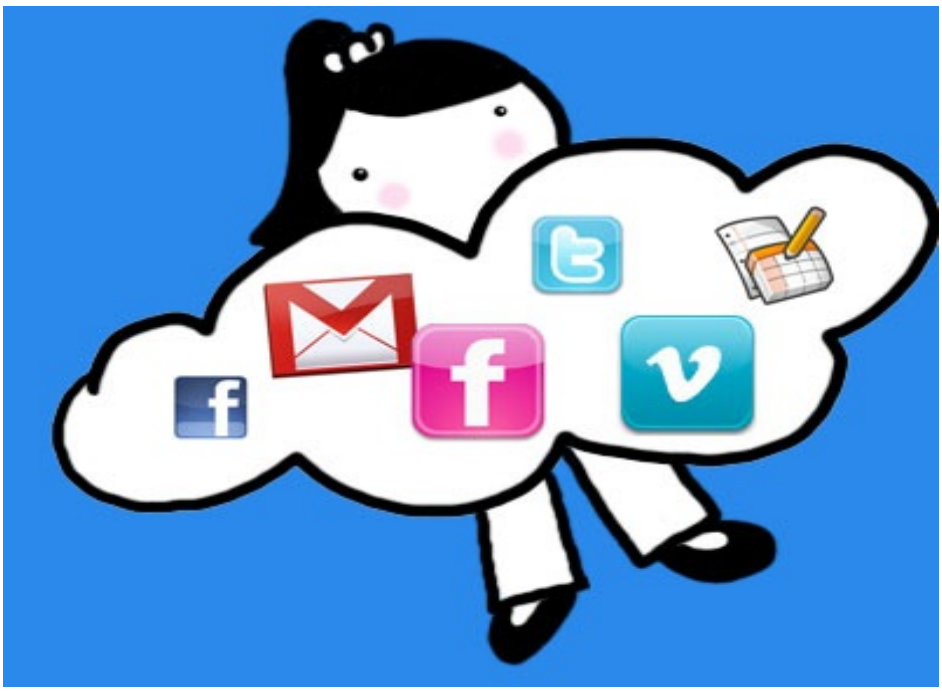
DONNÉES PERSONNELLES: ORAGE DANS LES NUAGES

LE 20 AVRIL 2010 ***NICOLAS KAYSER-BRIL***

Nicolas Kayser-Bril, qui s'occupe du datajournalisme ici chez OWNI, pige aussi aux Inrocks où il tient le blog Web-Obscur. Consacré aux arnaques et aux manipulations sur Internet, ses articles se penchent régulièrement sur les risques du cloud computing. Celui qui suit est une synthèse d'un article de février et de son follow-up d'avril.

Nicolas Kayser-Bril, qui s'occupe du datajournalisme ici chez OWNI, pige aussi aux Inrocks où il tient le blog ***Web-Obscur****. Consacré aux arnaques et aux manipulations sur Internet, ses articles se penchent régulièrement sur les risques du cloud computing. Celui qui suit est une synthèse d'un* ***article de février*** *et de* ***son follow-up d'avril*** *.*

—



Où sont mes données lorsque je les stocke en ligne sur Hotmail, Flickr ou Google Docs? Plusieurs affaires américaines sont venues souligner l'importance du problème ces derniers mois.

La complexité du statut juridique de données faisant plusieurs fois le tour du monde dans la journée et stockées sur des serveurs dans des endroits tenus secrets, fait qu'il est quasi-impossible d'évaluer précisément les risques posés par le *cloud computing*.

USA, Chine, Russie, France: Vos données ne se cachent plus

En août 2009, lors d'une enquête sur des spammeurs, le FBI a obtenu un mandat l'autorisant à exiger de Google de lui fournir tous les Google Docs d'un suspect (**voir l'article de *Wired***). 10 jours après, Google leur a envoyé les documents, dont une feuille de calcul contenait plus de 3 millions d'adresses spammées. Sans le *cloud computing*, obtenir une telle pièce à conviction aurait pris des semaines, puisqu'il aurait fallu aller la chercher sur le disque dur du suspect. Et encore, il aurait pu tout avoir effacé.

Le mieux dans cette histoire: **Le FBI n'avait même pas besoin de mandat**. Une loi de 1986, le **Stored Communications Act**, autorise la police à accéder aux documents personnels stockés sur un serveur après un délai de 180 jours. Ce qui était sensé dans les années 1980 (lorsque les documents ne faisaient que transiter du serveur vers des ordinateurs distants) provoque un joli maelström à l'heure de l'informatique dans les nuages.

En utilisant cette loi surannée, **un procureur général américain a voulu forcer Yahoo à**

transmettre des e-mails plus récents que 180 jours, sous prétexte que l'utilisateur les avait déjà lus (**toujours chez*Wired***).

Cette demande a provoqué une **levée de boucliers chez les défenseurs de la vie privée** outre-Atlantique. Soutenu par Google et l'Electronic Frontier Foundation, Yahoo a tenu bon, empêchant ainsi les flics US de lire à loisir les e-mails d'une vaste majorité d'Américains.

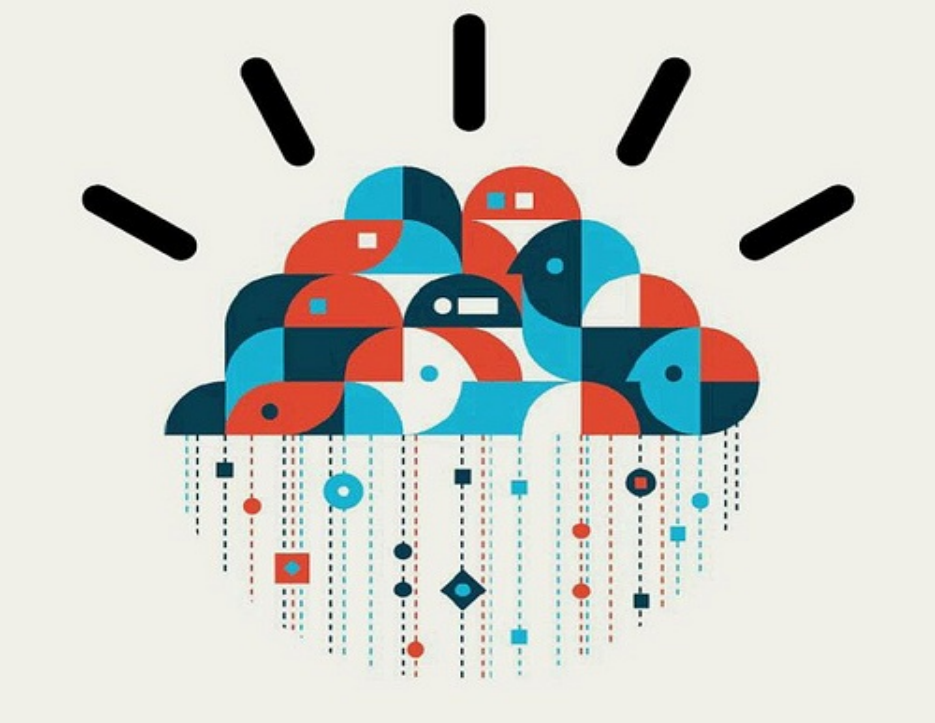
De l'autre côté du Pacifique, le 12 janvier dernier, **Google annonçait que le gouvernement chinois avait pénétré ses serveurs** et extrait des informations concernant les comptes Gmail de 2 opposants. Les fonctionnaires chinois seraient donc en mesure de s'introduire où bon leur semble dans les serveurs de Google.

Un peu plus à l'ouest, en 2007. **Microsoft annonce** l'ouverture prochaine d'un parc de serveurs à **Irkoutsk**, en Sibérie. Depuis, silence radio. Microsoft semble avoir levé le pied sur son investissement russe.

La raison? 4 mois après avoir signé un accord avec la **région d'Irkoutsk**, **le FSB (ex-KGB) est venu mettre son nez dans le dossier** en affirmant que si Microsoft n'était pas 100% transparent dans la manière de stocker les données, ses serveurs constituaient une menace pour la sécurité de l'État. En d'autres termes: Vous nous donnez l'accès à vos serveurs ou on ne vous laisse pas vous installer.

Retour en France pour finir, où en 2007, un médecin isérois partageant par mail avec ses collègues ses réserves quant au bien-fondé d'une mesure gouvernementale **s'est vu convoqué** chez le sous-préfet. Comment les e-mails se sont-ils retrouvés à la préfecture? Nul ne le sait.

Résultat, si vos données sont hébergées par un fournisseur basé aux États-Unis, ou même sur un serveur installé là-bas, la police n'a pas beaucoup d'obstacles à franchir pour y avoir accès. Si elles sont hébergées en Chine ou en Russie, le gouvernement n'a pas l'air de se gêner pour glaner ce qui l'intéresse. En France non plus, vos mails ne semblent pas protégés outre mesure.



Pourquoi tant de flou ?

En théorie, d'après la loi Informatique et Libertés de 1978, **chacun a un droit d'accès à ses données personnelles, ainsi que le droit de savoir si ses données sont envoyées en dehors de l'Union Européenne**. En réalité, i**l est très difficile de localiser des données en particulier**. Les géants du web, les Microsoft ou Google qui gèrent des dizaines de milliers de serveurs, équilibrent la charge entre leurs différentes 'fermes', de manière à pouvoir servir de manière optimale la partie du monde où les internautes sont éveillés.

Résultats, vos données peuvent être stockées en Belgique aujourd'hui et à Shanghai cette nuit. Difficile dans ces cas là de donner aux internautes une réponse définitive concernant la localisation de leurs fichiers. Je ne parle même pas des entreprises qui sous-traitent l'hébergement des données de leurs utilisateurs.

Le statut des données stockées dans les nuages manque de clarté. En France, la **loi relative au secret des correspondances électroniques** de 1991 dispose que la force publique ne peut mettre son nez dans vos mails que si la sécurité nationale est en cause (ou le grand banditisme, ou le terrorisme – le genre de choses qui a peu de chances de vous concerner). Et c'est le premier ministre qui doit autoriser et motiver l'autorisation d'espionner.

La **loi sur la confiance dans l'économie numérique** de 2004, qui devait éclaircir les choses, s'est bien gardée de trancher le débat. Elle définit l'e-mail mais en fait l'égal d'une lettre, ce que le conseil constitutionnel **a confirmé** par la suite. Pour les juges, les policiers et les citoyens, **le message est clair: Débrouillez-vous !**

Face à une loi aussi peu adaptée aux enquêtes ordinaires, c'est le flou qui domine. La distinction entre correspondance privée et professionnelle, par exemple, oscille depuis deux dizaines d'années. **Un jugement de janvier 2010** semble dire que les emails envoyés depuis le lieu de travail ne relèvent pas de la correspondance privée. Il vient à l'encontre **d'un jugement de 2001** qui disait exactement l'inverse, c'est-à-dire que toute correspondance électronique envoyée à un seul destinataire depuis une adresse protégée par mot de passe est privée. Jusqu'à ce que la cour de cassation tranche, les juges seront libres de se fonder sur l'une ou l'autre des décisions.

Un cocktail de lois nationales

Alors, faut-il préférer une loi Américaine qui ne protège que modérément l'utilisateur ou une loi française qui hésite depuis 20 ans sur la démarche à adopter? Et quels services sont soumis à quelles lois?

Dans **une décision d'avril 2008**, le TGI de Paris a affirmé que **les lois françaises ne s'appliquaient pas aux services hébergés aux Etats-Unis**. Les juges ont débouté une française exigeant que Google efface ses interventions sur Google Groups. Même s'ils ont souligné que **la loi de 1978**, censée donner aux internautes un droit d'accès à leurs données, ne s'appliquait pas à une entreprise californienne, les attendus expliquaient aussi que la plaignante pouvait faire le travail elle-même, en effaçant les messages à la main. Encore une fois, tant que la Cour de Cassation ne s'est pas prononcée, nul ne sait à quoi s'en tenir.

Mais de toute façon, une décision de justice en France peut très bien être contredite par un jugement américain. **Un article de Bloomberg** recense la flopée de jugements internationaux n'ayant aboutis à rien, faute de coordination entre juges européens et américains.

Pour Stéphane Grégoire, chargé de mission au **Forum des droits sur l'internet**, que j'avais interviewé en février, **la solution à ce méli-mélo juridique est d'unifier le droit du cloud computing au niveau mondial**. Les sites globaux, comme Facebook, sont soumis à 130 lois nationales différentes. Impossible dans ces conditions de créer des services sur mesure pour respecter les législations locales.

Dans ce but, le **groupe de travail G29**, qui rassemble les 27 CNIL européennes, propose pour commencer d'**unifier la notion de 'données à caractère personnel'** (**voir l'avis**). En effet, les textes communautaires laissent aux 27 membres de l'Union une bonne marge de manœuvre pour décider de l'interprétation de ce terme.

Pour une nouvelle approche du problème

La loi de 1978 se focalisait sur les données physiques et l'approche du législateur a peu changé depuis. A l'époque, il s'agissait de savoir si les cartes perforées, les bandes magnétiques et les disquettes seraient envoyées à l'étranger pour traitement. Et vu qu'un gigabit pesait une trentaine de kilos (stocké sur 320 **Commodore Datasette**, par exemple) contre un demi gramme aujourd'hui sur carte SD, il était plus facile de suivre les données à la trace.

Impossible à faire respecter aujourd'hui, **ces dispositions doivent être revues**. C'est ce qu'affirme Peter Fleischer, grand gourou de la vie privée chez Google. **Selon lui**, l'accès aux données est secondaire. L'important, c'est de savoir quelles sont les mesures prises pour les protéger, quelles sont les protocoles pour y accéder, etc. En effet, dans sa guerre de com' contre le gouvernement chinois, Google a révélé que la plupart des comptes Gmail compromis résultent de vols de mot de passes via des sites de **phishing**.

Le plus grand danger des sites communautaire ne vient pas d'une attaque extérieure, mais bien du voyeurisme des employés. **Chez Facebook, les employés peuvent voir quels sont les profils que vous consultez**. Loin d'en avoir honte, ils considèrent ça comme un des avantages du métier, **selon Valleywag**. C'était en 2007 et les choses ont sûrement

beaucoup changées depuis, mais les procédures de sécurité internes laissent souvent à désirer.

Quand elles existent.