

LES BIGS BROTHER DU WEB...

GAFAM... Google, Amazon, Facebook, Apple, Microsoft. Voici les 5 sociétés qui centralisent et proposent de très nombreux services que nous sommes amenés à utiliser de gré ou de force. Pourquoi ? Les smartphones que nous utilisons sont basés sur un système Android (Google), iOS (Apple) ou Windows (Microsoft).

Nous confions (donnons) donc à ces sociétés de très nombreuses informations sur notre vie. Localisation, emails, conversations sont ainsi analysés pour nous fournir une « meilleure expérience utilisateur » et « lutter contre le terrorisme ».

Côté meilleure expérience utilisateur ces sociétés se permettent alors de vendre des encarts de publicités à des annonceurs qui seront ciblées puisque celles-ci connaissent nos goûts.

Côté terrorisme, depuis l'affaire SNOWDEN (2013), nous savons que ces géants du web sont de communiquer des données privées (emails, conversations Skype, données de géolocalisation...) à des services gouvernementaux.

ALORS COMMENT DEVENIR PLUS ANONYME ?

Côté smartphone, difficile de trouver une solution alternative. Vous pouvez bien opter pour un smartphone basé sur un **système Linux**, <http://www.ubuntuphone.fr/> par exemple. Soucis, les applications sont beaucoup moins nombreuses que sur les plateformes (AppStore, PlaysStore, WindowsStore). Par ailleurs, vous devrez acheter ce smartphone sur Internet et contrairement aux smartphones proposés par votre opérateur vous devrez le payer cash !

Côté courriel par contre de nombreuses alternatives existent. Des adresses de courriels peuvent être créées chez certains fournisseurs (**Tutanota** par exemple) ou si vous en avez les compétences, vous pourriez héberger chez vous votre propre adresse de courriel.

Côté recherche sur Internet, vous pouvez utiliser un autre moteur de recherche que Google. **Duckduckgo** et **Qwant** ne conserveront pas vos d'informations sur vos recherches et ne vous proposeront pas de publicités ciblées.

Côté géolocalisation, vous pouvez sur votre smartphone **désactiver la fonction GPS**. Deux intérêts majeurs à cette désactivation... la société n'aura pas d'informations sur vos déplacements et les coordonnées GPS ne seront pas inscrites dans vos photos.

Si vous utilisez un appareil Android et que votre GPS est activé depuis un certain temps, vous pouvez aller voir sur <https://myactivity.google.com/> toutes les informations conservées par Google (déplacement, historique des recherches sur Internet, historique des recherches audio sur Google Play, Commentaires Youtubes...). N'hésitez pas à aller sur cette historique si vous utilisez un appareil utilisant un compte Google ou si vous utilisez le navigateur Google Chrome depuis votre ordinateur avec votre compte google régulièrement activé.

Côté ordinateur, le constat sera le même que pour les smartphones. Sauf si vous utilisez un ordinateur équipé d'un système Linux ou si vous avez installé un navigateur « libre » tel que Firefox et des logiciels libres (LibreOffice par exemple).

Et même si vous utilisez Firefox, vous devrez configurer celui-ci pour qu'il ne conserve pas votre historique, les cookies,..., voir les mots de passe. (allez dans le menu et choisissez options puis Vie privée).

Côté outils « web 2.0 », vous trouvez de très nombreuses alternatives aux outils Google, Microsoft, Apple sur le site de framasoftware dans la partie « Services libres ».

- Alternative à Skype... Framatalk,
- Alternative à Google Drive... Framadrive,
- Alternative à Google Agenda... Framagenda,
- Alternative à Doodle... Framadate,
- ...

Côté réseau sociaux... Difficile de faire l'impasse sur Facebook si vous souhaitez bénéficier d'un outils vous permettant de retrouver vos amis, anciens amis, connaissances éloignées. En effet, avec 30 millions d'utilisateur mensuels en France et 1,79 milliards dans le monde, vous ne trouverez pas d'outil comparable.

Maintenant si vous souhaitez développer votre propre réseau social, vous pouvez utiliser l'outil Whaller (c'est un outil Français) qui vous permettra d'inviter vos connaissances (amis, famille...) et de partager avec ceux-ci des informations plus privées. Enfin, si vous souhaitez toujours utiliser Facebook, vous pouvez en gérant vos paramètres de sécurité et en sélectionnant les lecteurs de vos « posts » mieux définir qui voit ce que vous publiez et quelles sont les informations visibles par tous.