Comment internet nous piste

Analyse d'un business florissant, où quand c'est gratuit, c'est vous le produit.

Par Virginie Jourdan. Illustration : Colcanopa

En négociant avec les sites

À chaque fois que nous naviguons sur un site, celui-ci dépose des «cookies» sur notre ordinateur (depuis 2011, tous ont l'obligation de le signaler à l'internaute). Ces petits paquets de lignes de code permettent au site et à notre machine de retenir identifiants, mots de passe, noms et dates de naissance inscrits dans un formulaire… Ils nous évitent de tout retaper à chaque visite. C'est aussi grâce à eux qu'apparaissent, sur des plates-formes comme Deezer ou YouTube, des suggestions d'artistes ou de vidéos susceptibles de nous plaire.
Le revers, c'est qu'ils savent presque tout de nous (heure de connexion, temps passé sur le site, goûts et habitudes de navigation…) et qu'ils ne le gardent pas pour eux! Les sites se servent en effet de ces cookies pour se financer. Ils autorisent des sociétés à récupérer, compiler et revendre ces infos à des publicitaires ravis de pouvoir mieux nous cibler.
Le marché de la pub sur Internet atteint près de 100 milliards d'euros par an.

La parade: limiter les cookies via les paramètres de «sécurité/confidentialité» d'Internet Explorer, Safari, Mozilla ou Google Chrome.

En lisant nos messages

Vous pensez que vos conversations sur Snapchat ou Gmail sont confidentielles? Pas du tout. La majorité des services de chat et de messagerie gratuits (Yahoo, Facebook, Hotmail…) le sont en échange de données sur nous. Pas seulement nos noms et dates de naissance mais aussi le contenu de nos messages: régulièrement, des robots repèrent, en quelques millièmes de secondes, la récurrence de certains mots et affichent des pubs en conséquence. Il n'y a donc rien de magique à ce que différents modèles de barbecue nous soient proposés alors qu'on a passé la semaine à échanger des mails entre amis pour en organiser un!

La parade: ouvrir un compte sur les messageries *no-log.org* ou *riseup.net*, gratuites, sécurisées et sans pub.

En étudiant nos profils

Facebook, par exemple, se sert de nos commentaires, photos, like et de nos amis pour cerner notre personnalité: centres d'intérêt, opinions, jusqu'à notre orientation sexuelle et notre propension à consommer des stupéfiants (si l'on utilise souvent le mot «herbe» ou «high»)! En fonction de ce portrait-robot, un algorithme va nous proposer des pages à aimer et des amis à accepter. Plus gênant: il va aussi préjuger de nos envies de lecture, mettre en avant certains posts et publications et évincer les autres de notre fil d'actualité. Ne nous donnant ainsi à voir qu'une toute petite partie du monde. Le risque? Une fermeture à d'autres idées que les nôtres et à tout ce qui ne nous ressemble pas. Et celui, encore plus grave, d'amplifier certains discours radicaux en faisant par exemple remonter sur nos fils toutes les publications et notifications concernant Dieudonné sous prétexte qu'on a laissé un commentaire ou un like sur sa page…

La parade: pour s'informer, consulter aussi des sites de médias fiables et généralistes comme *lemonde.fr, francetv.info* etc.

En scrutant nos recherches

Une recherche sur Biarritz, et voici que clignote un lien publicitaire vantant des planches de surf et autres bodyboards. Un hasard? Non. Google comme Yahoo search enregistrent et croisent en temps réel chaque terme utilisé lors d'une requête. Encore un coup des cookies et autres traceurs high-tech dont usent allègrement des moteurs de recherche pour nous connaître. Plus surprenant, ces aspirateurs de données analysent la configuration de nos ordinateurs: âge du système d'exploitation, logiciels installés, navigateur utilisé pour surfer sur Internet, adresse IP, marque et modèle de l'ordinateur… Cet examen garantit le bon affichage des pages. Mais des sites commerciaux s'en servent aussi pour présumer de nos moyens financiers: des études ont par exemple démontré que l'usage d'un ordinateur dernier cri provoque une hausse des tarifs des offres de voyage!

La parade: utiliser d'autres moteurs comme DuckDuckGo, Qwant ou Startpage qui ne collectent pas de données pendant les recherches.

En pillant nos smartphones

Données de géolocalisation, contacts, agenda… Toutes les applications installées sur nos téléphones captent, le plus souvent à notre insu, une foule d'infos nous concernant. Des infos encore plus intimes lorsque notre appareil est synchronisé avec un bracelet connecté qui relève notre pouls, notre temps de sommeil, nos calories…
Si les sociétés éditant ces applications s'en servent déjà pour se valoriser sur le marché (toutes ces datas constituent une richesse énorme), elles gardent le silence le plus total sur l'utilisation qu'elles pourraient en faire à l'avenir. Certains craignent qu'elles soient vendues à des clients comme les banques qui pourraient s'en servir pour sélectionner, par exemple, à qui elles accorderaient ou non un prêt étudiant…

La parade: lire les conditions générales d'utilisation des applis avant de les installer et aller dans «Réglages» pour limiter leur accès aux données du téléphone.