

Le pistage sur Internet

Beaucoup d'entreprises derrière les sites internet ont un modèle économique basé sur la publicité : l'utilisation est gratuite, et elles gagnent de l'argent en vendant de l'espace publicitaires à des annonceurs. Si les publicités sont ciblées, elles sont plus rentables donc ces entreprises cherchent à obtenir des informations sur leurs utilisateurs et utilisatrices (c'est à dire nous).

Les Cookies

Un cookie est un petit bout d'information stocké par notre navigateur par un site internet, et qu'on renvoie à chaque fois qu'on fait une requête à ce site. Cela permet notamment de rester connecté sur les sites avec des comptes utilisateurs.

Mais les cookies peuvent aussi être déposés par d'autres sites que celui qu'on visite si il y a dessus des éléments externes à charger (images, scripts) :

<!-- cette image est sur le même serveur que le site -->

<!-- alors que celle-ci est sur le site lemonde.fr, à qui on va devoir envoyer une requête pour l'afficher -->

Par exemple toutes les pages qui ont le bouton like de facebook créent une connexion à facebook, et comme on lui renvoie le même cookie à chaque fois facebook peut savoir qu'on est la même personne à être allée sur tous ces sites même si on ne clique pas sur le bouton.

Parfois l'image n'est même pas visible (un seul pixel transparent).

Comment empêcher le traçage par les cookies

Dans la plupart des navigateurs (Firefox, Chrome,...) on peut modifier les paramètres pour refuser certains cookies, par exemple tous les cookies tiers (qui viennent d'un autre site que celui qu'on visite).

On peut aussi utiliser une extension comme "Privacy Badger" (crée par l'association de défense des libertés Electronic Frontier Fondation) qui bloque certains éléments externes utilisés pour le pistage.

Bloquer les publicités

Il est possible de bloquer la plupart des publicités sur le web, par exemple avec l'extension "uBlock Origin" qui est libre et gratuite.

Il y a un débat sur le blocage de la publicité, qui peut mettre en danger le modèle économique de certains sites web, mais qui permet aussi de le rendre plus rapide (pas de chargement des publicités) et plus écologique (moins de ressources utilisées pour de la publicité).

Empreintes

Même si on bloque les cookies, il est difficile d'être vraiment anonyme sur un site web.

On a déjà vu dans la partie sur Internet que le site connaît notre adresse IP et donc une géolocalisation approximative (sauf si on utilise un proxy, VPN ou Tor).

Mais les requêtes http donnent encore plus d'informations, comme :

- le système d'exploitation, le navigateur web et sa version
- souvent la langue préférée et la taille de l'écran

Ces informations peuvent permettre aux sites d'envoyer une version de la page optimisée pour notre machine, mais elles peuvent aussi nous identifier partiellement si on est les seuls à avoir ces caractéristiques.

Il est possible de cacher ou modifier ces informations avec des extensions, mais on en donne toujours indirectement.

RGPD

Depuis 2018 le **règlement général sur la protection des données** renforce la protection des données personnelles. C'est notamment à cause de lui que les sites sont obligés de demander le consentement des visiteurs pour l'utilisation des cookies.