[Fiche 05] Les protections contre le tracage

Internet a de nombreux avantages, mais n'est pas sans défauts. La principale méthode de financement des sites Internet est la publicité. L'adage est connu "si c'est gratuit, vous êtes le produit". De nombreux sites vendent donc le "temps de cerveau disponible" de leurs utilisat·rices reportant les couts sur l'achat des produits ou services de l'annonceur. Au-delà du débat sur le bien-fondé de la publicité, celle-ci conduit souvent sur Internet au traçage de données personnelles. Ce traçage peut aller jusqu'au profilage détaillé des utilisat·rices, qui peut s'avérer extrêmement dangereux en termes de surveillance. En effet, pour optimiser les annonces, les sites collectent de nombreuses données qui servent autant :

- dans une approche générale, à identifier les profils des consommateurs potentiels,
- dans une approche individualisée, à proposer les publicités les plus susceptibles de conduire à l'acte d'achat.

C'est la principale source de revenus des deux géants Google et Facebook qui tirent la quasi-totalité de leurs revenus de la publicité et de l'exploitation des données personnelles. Ils représentent à eux deux autour de 50 % du marché publicitaire en ligne et ne cessent de croitre.

Les individus sont ciblés par ce biais en tant que consommateurs, parfois dans des proportions qu'ils n'imaginent pas. Leurs données peuvent également être exploitées à des fins de gestion ou de surveillance des populations. Les révélations Snowden ont montré que c'était le cas avec certains grands acteurs du numérique, notamment ceux souvent appelés les "GAFAM" (Google Amazon Facebook Apple et Microsoft).

.

Le problème est toutefois plus général notamment en raison des "courtiers en données" (*databrokers*) qui même s'ils sont moins connus accumulent et exploitent des quantités colossales de données personnelles. Certains de ces acteurs ne se contentent pas d'utiliser ces données pour des motifs commerciaux, mais n'hésitent pas à les utiliser dans des cadres politiques tels que des élections.

Cette surveillance en ligne est donc extrêmement problématique d'un point de vue économique comme démocratique.

Il existe pourtant une option présente dans les navigateurs qui vise à signifier aux sites visités que l'on ne souhaite pas être tracé, le "*Do Not Track*" (ne pas tracer). Sur Firefox :

> dans l'onglet "Vie privée" des options, cocher "Indiquer aux sites que je ne souhaite pas être pisté".

Malheureusement, il s'agit d'un projet de standard qui n'a pas abouti et la plupart des sites visités ne respectent pas ce souhait et au contraire cela peut leurs permettre de constituer des bases d'"internautes qui ne veulent pas être tracés". Le CECIL propose donc d'utiliser des outils plus protecteurs pour résister autant que possible à ces pratiques de traçage.

Il faut relever que Firefox protège, par défaut, contre certaines opérations de traçage, notamment en navigation privée et continue d'avancer en ce sens.

Pour compléter cette protection et l'améliorer, il est pertinent d'installer des modules qui vont bloquer au maximum les tentatives des sites pour obtenir des données sur l'utilisat·rice et l·a suivre dans ses navigations sur le Web.

uBlock Origin la star des "Adblock", contre le traçage publicitaire

Le plus célèbre d'entre eux est "Adblock Plus" qui fait disparaitre des navigations la majorité des encarts publicitaires. Toutefois en raison de ses nouvelles pratiques commerciales critiquables, le CECIL conseille plutôt d'installer uBlock Origin. Celui-ci ne comporte pas les fonctionnalités critiquées et est bien plus efficace et moins gourmand en mémoire.
Pour l'installer facilement sur Firefox, il suffit de l'ajouter *via* la plateforme d'extension de Firefox.

Il s'installe, par défaut, avec notamment une liste de base de publicités bloquées (*Liste-FR+EasyList*) qui va stopper la plupart des publicités sur Internet ainsi que la liste "EasyPrivacy" anti-traçage. Ces listes sont tenues à jour automatiquement et peuvent aussi être complétées. La sélection par défaut est efficace, mais pour en ajouter :

> Aller dans les préférences du module (Options – Modules – Préférences uBlock Origin), onglet "Listes de filtres" et activer les listes pertinentes (par exemple celles classées en "Confidentialité" et en "Réseaux sociaux").

Les listes "Fanboy's Anti-Thirdparty Social" et "Fanboy's Social Blocking List" sont importantes car elles bloquent les cookies dits "tiers" tels que ceux de Facebook, Google et Twitter, présents sur de nombreuses pages cachés derrière les boutons de "partage" (G+1, Like, Tw). Ceux-ci permettent à ces sociétés de connaitre les sites visités.

Il est aussi possible d'ajouter des blocages personnalisés. Par exemple, pour les utilisat·rices de Facebook, pour bloquer la fonctionnalité permettant aux participants à une discussion de voir si des messages ont été "vus", il faut aller dans l'onglet "Mes filtres" et ajouter :

> ||facebook.com/ajax/mercury/change_read_status.php$xmlhttprequest

Disconnect.me, en complément

Bien qu'uBlock Origin puisse bloquer les dispositifs de traçage, il n'est pas totalement destiné à cela et Disconnect.me reste un bon complément. Même si uBlock et Disconnect se recoupent partiellement, leurs listes de filtres ne sont pas identiques. Ainsi, Disconnect.me limite aussi les traçages d'analyse des consultations, ou des réseaux sociaux…

> Pour ajouter Disconnect.me à Firefox, aller sur la page de l'extension dans la base de Mozilla, puis "Ajouter à Firefox".

Pour compléter l'installation :

> Cliquer sur l'icône "D" de Disconnect.me et cliquer sur celle à côté de "Content" pour bloquer aussi les traqueurs contenus dans les articles (attention cela peut rendre certains contenus inaccessibles, il suffira de le décliquer pour ces contenus spécifiques).

Ces deux extensions protégeront contre un grand nombre de traqueurs.

Decentraleyes

De nombreux sites Internet font appel, par praticité à des ressources basiques stockées chez des sites tiers appelé des *"Content Delivery Network"* (CDN). Certains de ces CDN en profitent pour tracer les visiteurs de ces sites Internet. Decentraleyes va installer ces ressources basiques sur l'ordinateur et renvoyer les requêtes en local au lieu de permettre aux CDN de récupérer des données. C'est donc un complément intéressant pour limiter le traçage en ligne.

> Pour ajouter Decentraleyes à Firefox, aller sur la page de l'extension dans la base de Mozilla, puis "Ajouter à Firefox".

Privacy Badger, une protection dynamique de l'EFF

Privacy Badger, de l'Electronic Frontier Foundation, a pour objectif de combiner les avantages des différentes extensions protectrices de la vie privée (dont uBlock et Disconnect) au sein d'une seule extension. Il s'agit toutefois d'un projet récent et qui se consacre pour le moment principalement aux cookies traceurs. Il n'a pas pour vocation de bloquer les publicités qui ne tracent pas leurs utilisat·rices. Son fonctionnement est automatique et dynamique (il examine les actions d'une page pour savoir quoi bloquer), il n'est pas toujours évident de comprendre son impact, mais il peut constituer un module intéressant pour se protéger.

Ces modules sont une protection non négligeable, mais pour s'assurer qu'aucune requête ne sera suivie à travers le Web, d'autres précautions sont nécessaires.

Quelques autres extensions intéressantes

- En naviguant sur Internet, on transmet par défaut les caractéristiques du navigateur et du système d'exploitation. Pour le constater, on peut réaliser ou tester le "Panopticlick" de l'EFF. Pour éviter d'être trop transparent et choisir les informations transmises, on peut utiliser User

Agent Switcher. Ce module permet de faire croire que la requête provient, par exemple, d'une vieille version d'Internet Explorer ou d'un robot d'indexation de contenu de Google.
    - Le module Lightbeam de la Fondation Mozilla permet de prendre visuellement conscience de certaines opérations de traçage en ligne.
- HTTPS Everywhere, de l'Electronic Frontier Fondation, vise à faire transiter les communications de façon chiffrée dès que cette option est disponible et réduit ainsi les risques d'écoutes.
- Signalons aussi Self Destructing Cookies, qui permet de se débarrasser des cookies générés par une page dès que celle-ci est fermée évitant ainsi que ces cookies soient ultérieurement consultés.
- Pour les utilisat·rices plus avisé·es et prêt·es à réaliser les configurations nécessaires (souvent gérer les autorisations site de confiance par site de confiance), il est enfin recommandé d'utiliser uMatrix.

Pour aller plus loin :

- pour connaitre les traces basiques, mais nombreuses laissées lors des navigations : visiter le site What every Browser knows about you, le jeu en ligne Clickclickclick est aussi éloquent à cet égard.
- La page "contrôle tes données" gérée par la Quadrature du Net,
- un article d'Aeris sur son blog, Extensions Firefox pour protéger sa vie privée 2015-12-08,et de D. Crawford sur bestvpn en anglais, *The Complete Firefox Privacy and Security Guide*, sur les extensions relatives spécifiquement à la sécurité sur Firefox.

La plupart des extensions précédemment mentionnées, et notamment uBlock Origin permettent d'exclure ou d'inclure certains éléments du filtrage. On parle de "liste bloquée" ou de "liste autorisée". Ainsi, si on souhaite permettre à un site de nous tracer on peut choisir de désactiver le blocage sur ce site en particulier (liste autorisée).

> Pour cela cliquer sur le logo d'uBlock Origin et cliquer sur le "Symbole bleu" pour désactiver (ou réactiver) le blocage.

À l'inverse, si certains éléments ne sont pas automatiquement bloqués par les listes installées on peut les bloquer spécifiquement (liste bloquée).

> Pour cela, réaliser un clic droit sur l'élément souhaité et cliquer sur "Bloquer cet élement".

- Voir également la page de la CNIL «Maitriser mes données» sur son site cnil.fr.
- Pour comprendre le fonctionnement de Decentraleyes, voir leur Foire aux questions.

Sur la question du "Do Not Track", voir :

- la page du projet : donottrack.us (en anglais),
- une explication sur le site de l'EFF, "Do not Track" (en anglais),
- la page Wikipedia française "Do Not Track".

Fiche 5 [publiée le 2 avril 2015, dernière mise à jour avril 2018]

degooglisons-internet.org