Quelques notions de cybersécurité

À destination des masterant·es et doctorant·es de l'EUR Sciences sociales du genre et de la sexualité

Christelle AVRIL – Février 2022

Table des matières

1. Pour protéger vos données personnelles et celles de vos enquêté·es

Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) utilisent les données que vous mettez sous leurs outils, les diffusent, voire les revendent.

Elles sont stockées sur des serveurs qui se trouvent dans des pays qui ne sont pas soumis au RGPD (hors Europe).

Elles mettent en rapport vos données (celles de Facebook peuvent être appariées avec celles d'Amazon, etc.).

En dehors des GAFAM, il existe des attaques contre votre vie privée et des vols de données dont vous devez apprendre à vous protéger.

- ⇨ Pour limiter le pouvoir des GAFAM et protéger vos données ainsi que celles de vos enquêté·es, une solution consiste à apprendre à **compartimenter** vos activités et à **diversifier** les outils que vous utilisez en essayant autant que possible de remplacer ceux des GAFAM par des alternatives.
- ⇨ Pour protéger vos données ainsi que celles de vos enquêté·es des GAFAM, mais aussi des différentes attaques du web, une solution consiste à paramétrer correctement vos ordinateurs et téléphones mobiles, ainsi que toutes les applications, navigateurs, etc. que vous utilisez.

2. Compartimenter et diversifier tous vos outils

Utilisez des outils différents de vos systèmes (Microsoft, Apple) pour naviguer sur internet ou pour réaliser votre travail. Cela vaut pour vos ordinateurs comme pour vos téléphones.

NB : l'idéal serait en réalité d'utiliser un autre système que Windows ou Apple, comme Linux par exemple. Les conseils ci-dessous concernent les personnes qui n'utilisent pas d'autres système d'exploitation de leur ordinateur ou de leur téléphone que ceux déjà installés par Microsoft, Android et Apple.

Pour votre navigateur : Préférez des outils alternatifs : Tor, Firefox, Brave, Chromium, etc.

Pour votre moteur de recherche : sous Firefox par exemple, le moteur de recherche par défaut est Google. Dans les paramètres de votre navigateur, vous pouvez changer le moteur de recherche. Vous pouvez par exemple utiliser Duckduckgo, Qwant, etc.

Pour vos applications bureautiques, etc. : vous n'êtes pas obligé·e d'utiliser les applications de traitement de texte ou de calcul de Microsoft ou Apple. Il existe des applications « open source » et libres : voir sur Framasoft, Freesoftware Foundation, etc. Vous y trouverez le pack Libre Office ou encore des antivirus.

Pour votre messagerie électronique (compte e-mail) et certaines applications : l'EHESS met à votre disposition une messagerie institutionnelle sécurisée, ainsi que des outils sécurisés sur l'ENT (pour les questionnaires, les sondages, le partage de documents, etc.). Privilégiez les outils institutionnels pour votre vie professionnelle/étudiante et créez des adresses sur d'autres supports pour votre vie personnelle, pour les achats en ligne et les marques qui vous demandent une adresse de messagerie. Par exemple, vous pouvez vous créer une adresse de messagerie pour les marques comme Nom.achats@gmail.com

Vos mots de passe : changez vos mots de passe et ne les pré-enregistrez pas sur vos applications. Vos pouvez les conserver dans un tableur (Libre Office Calc, Excel, etc.) crypté ou au moins verrouillé par un mot de passe. Deux techniques pour les mots de passe : aller sur un générateur de mot de passe. Ou bien modifier à la marge un mot de passe habituel (en ajoutant à chaque fois au début et/ou à la fin, des signes, des chiffres, des majuscules, etc.)

Vos réseaux sociaux : pour les enquêtes de terrain, les données sensibles, privilégiez les réseaux cryptés comme Signal ou au moins les SMS (les données n'y sont pas aspirées et vendues comme sur les réseaux sociaux des GAFAM). Il existe une initiative qui vise à contrer la mise en commun de vos données (Facebook, Twitter, YouTube, Pinterest, etc.) sur un serveur unique, c'est le Fediverse. Le Fediverse propose des applications alternatives à Facebook, Pinterest, Spotify et Deezer, etc. et les données de ces applications sont stockées sur des serveurs distincts tout en pouvant être mises en lien selon un système de fédération de serveurs (et non plus de centralisation). ➔ Fediverse organise des formations (les Fediverse party), vous pouvez aller consulter leur site : ➔ https://fediverse.party/

3. Entretenir et paramétrer les outils

Que vous utilisez les outils des GAFAM ou d'autres, il faut prendre le temps de mettre à jour les outils et d'examiner tous les paramètres, notamment de décocher les nombreuses conditions cochées par défaut.

Paramétrer et entretenir les systèmes et logiciels

- L'antivirus : vous devez impérativement avoir un antivirus sur votre ordinateur (pour l'instant, c'est relativement inutile sur votre téléphone). Si vous utilisez Windows 10, il existe à présent un antivirus performant dans le système mais encore faut-il vérifier qu'il est activé. Si vous branchez une clé USB sur votre ordinateur, vérifiez aussi qu'elle ne se met pas automatiquement en route mais que l'antivirus l'examine avant (en cherchant sur internet, vous trouverez des tutos pour toutes ces questions). Si vous n'avez pas Windows 10, allez voir sur les site open source et libre, pour télécharger un antivirus.
- Le système de votre ordinateur ou de votre téléphone doivent être verrouillés par un mot de passe.
- Il faut faire les mises à jour système et pilote de logiciels, applications, etc. Ces mises à jour servent à vous protéger efficacement contre les virus en constante évolution.

Paramétrer correctement tous vos outils

- Tous les outils que vous utilisez sont paramétrés de manière à capter le maximum de données personnelles. Vous devez donc prendre le temps de modifier ce paramétrage. Et notamment de décocher nombre de conditions que vous avez acceptées sans le savoir. Sur internet, vous trouverez des tutos ou site web qui vous expliquent comment protéger vos données application par application. Il s'agit ici des applications sur ordinateurs, mais aussi sur vos téléphones. Sur ces derniers, il est plus difficile de se protéger, certaines fonctionnalités disponibles sur ordinateurs sont introuvables sur les téléphones. Néanmoins, on peut toujours supprimer les cookies, la géolocalisation, l'enregistrement automatique des données bancaires, etc.

- Un paramétrage minimal concerne vos données de navigation : vous pouvez faire en sorte de ne laisser aucune trace en termes d'historique, de cookies, etc.
- Exemple avec Firefox :
    - dans Paramètres, allez dans Vie privée et sécurité. Changez les paramètres de navigation : cocher la navigation personnalisée et cocher tous les blocages : cookies, etc. Firefox va vous dire que ça risque de limiter votre accès à des sites mais en réalité, si c'est le cas, Firefox vous demandera si vous faîtes une exception pour tel ou tel site quand vous allez sur l'un de sites concernés. Il n'y a donc aucun blocage dont vous n'ayez connaissance.
    - Cocher « toujours » envoyer un signal aux sites de ne pas me pister.
    - Cookies : cocher supprimer les données de site et cookies à la fermeture du navigateur.
    - Ne pas enregistrer vos mots de passe et identifiants.
    - Historique : navigation privée (donc aucun cookies).
    - Permissions : bloquer les fenêtres pop-up, prévenir quand les sites essaient d'utiliser des modules complémentaires.
    - Ne pas autoriser la collecte des données par Firefox : donc décocher « autoriser », …
    - Sécurité : bloquer les contenus dangereux, etc.

⇨ Firefox fonctionne tout à fait normalement malgré ces protections et contrairement à ce qu'on essaie généralement de vous faire croire. Vous pouvez faire la même chose avec le navigateur sur votre téléphone (en évitant chrome et en utilisant plutôt Brave ou autre avec un moteur de recherche qui n'est pas Google, etc.) à la condition de bien « quitter » le navigateur en partant.

- Vous pouvez de la même manière, vous protéger a minima sur les réseaux sociaux en verrouillant les accès publics, etc.

4. Quelques Ressources à compléter

CNIL, Dossier « Cybersécurité », https://www.cnil.fr/fr/cybersecurite

ANSSI, MOOC « SecNumacadémie », https://secnumacademie.gouv.fr/

Pix, https://pix.fr/

Marc Meillassoux, « Disparaître. Sous les radars des algorithmes », LuFilms, 2021, diffusé sur arte : https://www.arte.tv/fr/videos/100750-000-F/disparaitre-sous-les-radars-des-algorithmes/

➔ Si vous souhaitez compléter ce document, les ressources possibles (tutos, etc.), apporter d'autres pistes, voici un fichier partagé pour le faire : https://annuel2.framapad.org/p/2daebd4s3s-9snl?lang=fr