

Petit guide de liberté numérique

C'est un fait, nos activités en ligne sont désormais amplement surveillées et enregistrées par des sociétés privées et des états.

L'agenda des mondialistes et transhumanistes en tout genres n'est jamais bien loin de l'ombre des GAFAM et autres géants de la Silicon Valley qui cherchent à tout prix à digitaliser nos existences.

Dans un monde en pleine mutation, peut-être demain encore plus qu'aujourd'hui, notre vie privée doit rester un droit et une liberté fondamentale.

Comme je dispose d'une certaine agilité dans ce domaine, l'idée m'est venue de partager quelques informations importantes à ce sujet. Je résume dans ce bref courrier des éléments qui sont détaillés avec brio sur www.pypo.eu, un site dédié à nous permettre de nous soustraire aux regards indiscrets qui traquent nos moindres faits et gestes sur internet.

Quelques faits et solutions simples :

Google, Apple Facebook, Amazon, Microsoft, etc.

Ce n'est plus un secret pour personne : les géants du net utilisent des technologies de pistage sans votre consentement, enregistrant avec précision où vous êtes, qui vous êtes et ce que vous faites, 24 heures sur 24, 7 jours sur 7. Nos smartphones et ordinateurs sont devenus essentiellement des dispositifs de surveillance collectant et partageant vos données personnelles au plus offrant.

Très souvent, *"si c'est gratuit, c'est vous le produit."*

Notre identité numérique est profilée, analysée, vendue, partagée sans vergogne à des fins publicitaires. L'actualité regorge de scandales de fuites de données personnelles. Gmail analyse en permanence les contenus de nos emails ([ici](#)). Facebook laisse fuir les données de 267 millions de comptes ([ici](#)). WhatsApp va désormais partager plus de données avec sa maison mère ([ici](#)). La liste est longue, et nous rapproche un peu plus, souvent à notre insu, d'un monde orwellien.

Par exemple, savez-vous que Google Maps garde un historique de tous vos déplacements et positions via le GPS de votre téléphone, et ce depuis toujours ? Pour désactiver cette fonctionnalité activée par défaut, c'est par [ici](#).

Que faire ?

Reconquérir notre vie privée n'est pas facile, mais c'est possible. Dans un sens, il est déjà « trop tard », nos données personnelles ont été accumulées pendant des années. Remettre les compteurs à zéro est presque illusoire tant l'ingénierie numérique est tentaculaire. Par contre, il est possible d'arrêter les frais.

Il s'agit de changer ses habitudes et de faire le tri. Cela prend du temps, mais cela vaut la peine. Un niveau très élevé de sécurité est indispensable pour les journalistes et les lanceurs d'alertes par exemple, mais pour le commun des mortels, ce n'est sans doute pas nécessaire.

Dans un climat où la pensée unique tend à s'imposer et où le contrôle numérique est présenté comme l'unique voie possible, la résistance, la dissidence peuvent nécessiter à tout le moins de s'assurer que les communications privées restent...privées. Plusieurs opérations peuvent être réalisées simplement. Je vous les présente dans l'ordre, classées par facilité de réalisation.

1. Utilisez un bloqueur de publicités (facile - 3 min)

Du point de vue de la confidentialité, les publicités en ligne sont un cauchemar. Les annonces sont généralement diffusées via des domaines tiers (réseaux de publicité) et contiennent un suivi sophistiqué.

Le logiciel de suivi intégré aux annonces est utilisé pour créer un profil d'utilisateur unique incluant vos centres d'intérêt, votre activité de navigation, votre localisation, votre âge, les membres de votre famille, vos amis, etc. En fonction de votre profil d'utilisateur, des annonces ciblées vous seront diffusées via les réseaux de publicité des sites Web que vous visiterez. Les publicités sont comme des caméras de surveillance numériques qui violent constamment votre vie privée. (Source : www.pypo.eu)

Que faire ? C'est facile : ajouter une extension à votre navigateur web :

- [uBlock Origin](#) : facile à installer et bloque un large spectre de publicité et de suivi

2. Changer de navigateur et de moteur de recherche (facile - 10 min)

Google est le champion du profilage publicitaire : toutes vos recherches, vos déplacements, vos achats en ligne, etc. alimentent votre « profil numérique ». De plus, la majorité des sites installent des « mouchards » sur votre ordinateur, gentiment appelés « cookies ».

Utilisez de préférence (pour votre ordinateur et pour votre smartphone) :

- [Brave Browser](#) : bloque les cookies, les publicités et les traceurs.
- [Firefox](#) : navigateur grand public le plus respectueux de la vie privée

Concernant le moteur de recherche, fuyez Google qui donne des résultats partiels, enregistre et revend tout ce qui est possible et imaginable sur votre vie numérique et préférez :

- [Startpage](#)
- [Qwant](#)
- [Ecosia](#) (pas vraiment orienté vie privée, mais déjà mieux que Google)

Après avoir installé votre nouveau navigateur, rendez-vous dans les paramètres pour changer le moteur de recherche par défaut.

Plus d'infos sur les navigateurs web [ici](#) et sur les moteurs de recherche [ici](#).

3. Quitter WhatsApp et Messenger (moyen - 15 min)

Récemment, WhatsApp a fait la une de l'actualité avec la mise à jour de sa politique de confidentialité. Beaucoup se sont tournés vers Telegram, mais à en croire l'analyse de www.pypo.eu, il serait plus judicieux de se tourner vers [Signal](#), plus sécurisé et n'offrant pas de porte dérobée aux gouvernements.

Comme pour le changement d'adresse email, cela peut sembler pesant : tout le monde utilise WhatsApp. La solution est de définir un statut dans votre WhatsApp indiquant que vous ne communiquez plus via ce canal, ou de copier/coller un message informatif à ce sujet à vos proches qui souhaitent vous contacter.

4. Choisir une alternative à Gmail, Outlook et Yahoo pour les emails. (long - 45 min)

Les emails ne sont ni privés, ni sécurisés. Nos courriels sont largement épiés par des algorithmes et des institutions. Les documents déclassés du [programme de surveillance PRISM](#) révèlent que de nombreux grands fournisseurs de courrier électronique accordent aux agences de surveillance américaines un accès unilatéral à leurs serveurs pour effectuer «une surveillance étendue et approfondie des communications en direct et des informations stockées».

Les alternatives sont nombreuses, bien que la solution parfaite n'existe pas, et leur niveau de confidentialité dépend en partie de la juridiction du pays où elles sont établies, ainsi que de leurs choix technologiques. De toute manière, c'est toujours largement mieux que Gmail.

- [Mailfence](#) en Belgique
- [Tutanota](#) en Allemagne
- [ProtonMail](#) en Suisse (remis en question depuis qu'ils ont accepté un « investissement » américain de 2 millions de dollars...)

C'est sans doute l'étape la plus laborieuse : changer d'adresse email. Pratiquement, le plus simple est de configurer un message d'absence automatique pour avertir tous vos contacts qui vous écriront à l'avenir que vous utilisez désormais une autre adresse email.

Pour configurer un message automatique sur Gmail par exemple, voici les infos [ici](#).

Après un certain laps de temps, on peut alors penser à [supprimer son compte Gmail](#) et toutes les données qu'il contient, après avoir sauvegardé l'essentiel (contacts, emails importants...)

5. Utilisez un gestionnaire de mot de passe (facile - 10 min)

Plutôt orientés sur la question du piratage de comptes (qui peut se transformer rapidement en cauchemar onéreux dans le cas de demande de rançon ou de chantage, notamment dans le cadre de l'entreprise), les gestionnaires de mot de passe permettent d'utiliser automatiquement des mots de passe sécurisés et de ne plus se soucier de devoir les retenir.

Combien de fois n'ai-je pas vu des personnes oublier leur mot de passe, ou utiliser le même partout ? Personnellement, l'utilisation de Dashlane m'a vraiment facilité la vie sur le net. Je vous le recommande vivement !

- [Dashlane](#)
- [Lastpass](#)

6. Utiliser un VPN (avancé - 45 min)

Si vous voulez pousser la chansonnette, utilisez un VPN (pour Very Private Network), qui permet de masquer votre adresse IP et votre géolocalisation. Service payant. Pour les personnes ayant réellement besoin de plus de sécurité sur internet (vie professionnelle, lanceurs d'alerte, etc.).

7. Quitter les réseaux sociaux (Facebook, Instagram etc.) (avancé - 2h)

Bien que ce soit un choix (malheureusement) devenu « social », c'est un pas important dans la reconquête de la vie privée. Personnellement j'ai quitté Facebook il y a 2 mois, et je ne m'en porte que mieux. Par contre, ça m'a pris 3 jours. En effet, Facebook ne supprime pas vos données si vous supprimez votre compte. Il faut supprimer manuellement ses publications et photos. Explications en détail [ici](#).

8. Paramétrer correctement vos appareils (moyen - 15 min)

Windows est une vraie plaie pour la vie privée, et les options par défaut doivent vraiment être paramétrées. Mac offre un meilleur niveau de sécurité, mais a aussi besoin d'être paramétré. A-t-on vraiment besoin d'être géolocalisé à 1m près à chaque fois que l'app de météo se connecte à internet ?

- Guide pour Windows : <https://pypo.eu/je-securise-mon-pc/>
- Guide pour Mac : <https://pypo.eu/je-securise-mon-macbook-imac/>

Et idem pour les smartphones :

- iPhone : <https://pypo.eu/je-securise-mon-iphone/>
- Android : <https://pypo.eu/je-securise-mon-telephone-android/>