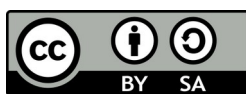


Guide de Souveraineté Numérique

46 Fiches Pratiques pour reprendre le contrôle de vos données

Version 2.4 – Juin 2026



<https://creativecommons.org/licenses/by-sa/4.0/>

gabriel.ananda@mailo.com



Table des matières

Introduction

[Petite histoire de notre liberté numérique et pourquoi ces fiches sont une nécessité](#)

⇒ [Petit guide pour comprendre l'informatique sans se prendre la tête](#)

⇒ [Analyse des dépendances des fiches pratiques de souveraineté numérique](#)



Bureautique et logiciels (remplacer Microsoft Office, Google Docs, Adobe)

[Fiche N°1 – Libérez-vous des suites bureautiques propriétaires](#)

[Fiche N°23 – Outils libres de retouche photo \(GIMP, Darktable, RawTherapee\)](#)



Navigateurs et vie privée (remplacer Chrome, Edge, Safari)

[Fiche N° 2 – Naviguez sans être pisté \(protection de base\)](#)

[Fiche N°11 – Naviguez sans être pisté \(protection avancée\)](#)

[Fiche N°14a – Nettoyez vos liens partagés](#)

[Fiche N°14b – Cas particuliers du nettoyage de liens partagés](#)

[Fiche N°41 – Raccourcissez vos URLs en souveraineté numérique](#)



Moteurs de recherche (remplacer Google Search, Bing)

[Fiche N°17 – Utilisez un moteur de recherche qui ne vous traque pas](#)



Messagerie éthique (remplacer Gmail, Outlook, Yahoo, iCloud)

[Fiche N°10 – Messagerie email éthique](#)

[Fiche N°36 - Auto-hébergement mail pur](#)



Messageries instantanées (remplacer WhatsApp, Messenger, Telegram, Signal)

[Fiche N°15 – Messageries instantanées cryptées sans numéro de téléphone](#)

[Fiche N°33 - Element / Matrix – Guide détaillé](#)



Cloud, stockage et synchronisation (remplacer Google Drive, iCloud,

OneDrive, Dropbox)

[Fiche N° 7 – Alternatives libres à Google Drive et Google Doc](#)

[Fiche N°29 – Synchronisez vos appareils sans Cloud avec Syncthing](#)

[Fiche N°31 – Utilisation d'un NAS pour centraliser et sauvegarder vos données](#)

[Fiche N°34 - Nextcloud – Auto-hébergement pas à pas \(votre propre cloud privé\)](#)



Sécurité, mots de passe et chiffrement

[Fiche N°16 – Gestionnaires libres de mots de passe](#)

[Fiche N°18 – Authentification à deux facteurs \(2FA\) pour plus de sécurité](#)

[Fiche N°26 – Chiffrez vos fichiers sensibles](#)

[Fiche N°35 - Vaultwarden – Auto-hébergement Bitwarden \(gestion de mots de passe\)](#)

[Fiche N°37 - Vérifier l'intégrité des fichiers avec GPG \(signatures, checksums\)](#)

[Fiche N°40 - Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur](#)



Cartographie (remplacer Google Maps, Waze, Apple Plans)

[Fiche N°24 – Outils de cartographie sans pistage](#)



Vidéo et streaming (remplacer YouTube)

[Fiche N°3 – Utilisez YouTube sans publicités](#)

[Fiche N°25 – Publiez des vidéos sans YouTube avec Peertube](#)



VPN, DNS et protection réseau

[Fiche N° 4 – Installez et utilisez Proton VPN \(version gratuite possible\)](#)

[Fiche N° 5 – Installez et utilisez Mullvad VPN \(version payante uniquement\)](#)

[Fiche N° 6 – Changez votre serveur DNS pour plus de confidentialité et de sécurité](#)

[Fiche N°30 – Sécurisez la porte d'entrée de votre réseau \(mise à jour de votre box\)](#)

[Fiche N°38 - Installez Pi-hole sur Raspberry Pi ou vieux PC – Bloquez les publicités au niveau de votre réseau](#)



Désintoxication numérique (quitter les big tech)

[Fiche N° 9 – Désactivez les fonctions Cloud des Big Tech](#)

[Fiche N°12 – Renoncer progressivement aux outils Big Tech](#)

[Fiche N°13 – Libérez vous de Windows ou MacOS et passez à Linux](#)

[Fiche N°39 - Nettoyer son empreinte numérique](#)



Sondages et formulaires (remplacer Google Forms, Doodle)

[Fiche N° 8 – Alternatives libres à Doodle](#)



Auto-hébergement et serveurs personnels

[Fiche N°20 – Auto-hébergez vos services avec Yunohost](#)

[Fiche N°28 – Choisissez un hébergeur web européen et éthique](#)



Anonymat et sécurité extrême

[Fiche N°27 – Apprenez à surfer anonymement avec Tor Browser](#)

[Fiche N°32 - Installation et utilisation de Tails - Naviguez sans laisser de traces](#)



Sauvegardes (remplacer iCloud Backup, Google Backup)

[Fiche N°19a – Sauvegardez vos données sous Linux Mint](#)

[Fiche N°19b – Sauvegardez vos données sous Windows](#)

[Fiche N°19c – Sauvegardez vos données sous macOS](#)

[Fiche N°19d – Sauvegardez vos données sous Android](#)

[Fiche N°19e – Sauvegardez vos données sous IOS-IPhone](#)



Agrégateur RSS (remplacer les réseaux sociaux et newsletters)

[Fiche N°21 – Reprenez le contrôle de votre fil d'actualités avec un agrégateur RSS](#)



Réseaux sociaux (remplacer Twitter, Facebook, Instagram)

[Fiche N°22 – Rejoignez le Fédiverse sans algorithme ni pub \(Mastodon / Bluesky\)](#)

Classement par niveau de difficulté

Niveau	N° des fiches
★☆☆☆☆ (Très facile)	N°2, N°3, N°8, N°14a, N°17, N°29, N°30
★★☆☆☆ (Facile)	N°1, N°4, N°6, N°7, N°9, N°10, N°11, N°12, N°13, N°14b, N°15, N°16, N°18, N°19a-e, N°21, N°22, N°24, N°26, N°27, N°31, N°32, N°39, N°46
★★★☆☆ (Moyen)	N°5, N°20, N°23, N°25, N°28, N°33, N°34, N°35, N°37, N°38, N°40
★★★★☆ (Avancé)	N°36



Suggestions de lecture par profil

Vous êtes...	Commencez par les fiches...
Débutant	N°1 (bureautique) → N°2 (navigateur) → N°3 (YouTube) → N°10 (email) → N°16 (mots de passe) → N°46 (frly.eu)
Famille / particulier	N°10 (email) → N°15 (messaging) → N°24 (cartographie) → N°31 (NAS) → N°46 (frly.eu)
Entreprise / association	N°20 (Yunohost) → N°28 (hébergeur) → N°25 (Peertube) → N°33 (Matrix) → N°40 (BIOS/UEFI) → N°46 (URLR)
Militant / journaliste	N°27 (Tor) → N°32 (Tails) → N°15 (SimpleX) → N°18 (2FA) → N°39 (empreinte numérique) → N°40 (BIOS/UEFI)
Exigeant / paranoïaque	N°5 (Mullvad) → N°36 (mail pur) → N°37 (GPG) → N°38 (Pi-hole) → N°35 (Vaultwarden) → N°40 (BIOS/UEFI) → N°46 (YOURLS)
Curieux de Linux	N°13 (Linux) → N°20 (Yunohost) → N°34 (Nextcloud) → N°40 (BIOS/UEFI)

Petite histoire de notre liberté numérique et pourquoi ces fiches sont une nécessité

Il fut un temps, pas si lointain, où Internet ressemblait à une immense bibliothèque et à une place publique à la fois. Un endroit où l'on partageait des connaissances, des fichiers, des idées, sans avoir à se demander qui écoutait, qui regardait, qui analysait. C'était l'époque des débuts du web : des forums, des blogs personnels, des pages web montées à la main, des logiciels libres échangés par passion. L'internaute était un acteur, un contributeur, parfois même un anonyme parmi d'autres anonymes.

À cette époque, l'utopie du réseau était simple : **tout le monde pouvait parler à tout le monde, sans intermédiaire, sans surveillance, sans marchand.**

L'âge d'or (naïf) de la liberté numérique

Le protocole TCP/IP, le World Wide Web de Tim Berners-Lee, les premiers navigateurs... tout avait été pensé pour l'ouverture et la décentralisation. On croyait (on voulait croire) que la technique, par nature, protégeait les individus. Les moteurs de recherche eux-mêmes se voulaient de simples index, pas des profilers.

C'est dans ce contexte qu'est née une génération d'internautes qui pensait que le réseau serait un rempart contre l'autorité et le commerce de masse.

La marchandisation : vous n'êtes plus un internaute, vous êtes un produit

Cette époque idyllique n'a pas duré. Très vite, quelques entreprises ont compris une chose fondamentale : **l'attention et les données des utilisateurs valent de l'or.**

Google, Facebook (Meta), Amazon, Microsoft, Apple n'ont pas gagné parce qu'ils avaient les meilleurs services, mais parce qu'ils ont transformé l'internaute en client potentiel permanent.

Chaque clic, chaque recherche, chaque vidéo regardée, chaque email lu est devenu une matière première pour construire un **profil ultra-précis** : vos opinions, vos faiblesses, vos désirs, vos habitudes, vos fréquentations. On ne se contente plus de vous proposer un service ; on vous invente des besoins, on vous pousse à la consommation, on vous enferme dans une bulle algorithmique.

Vous n'êtes plus libre. Vous êtes **prédictible**.

Les big tech ont capturé la quasi-totalité des usages quotidiens : la recherche web, la messagerie, le stockage de fichiers, la cartographie, les réseaux sociaux, la vidéo, la bureautique... Parfois gratuitement, parfois en échange de vos données, parfois en payant un abonnement... mais en restant toujours sous leur regard.

La surveillance de masse : quand les États s'en mêlent

Dans le même temps, les gouvernements – y compris ceux qui se disent démocratiques – ont compris l'intérêt stratégique de ce gigantesque mouchard.

Le **Cloud Act** américain permet à Washington de réquisitionner des données stockées... même en Europe, si la maison mère est américaine.

En France, en Allemagne, ailleurs, les lois sur le renseignement se sont élargies. Les fournisseurs d'accès sont mis à contribution. Les box, les routeurs, les OS propriétaires (Windows, macOS, Android, iOS) sont devenus des portes dérobées potentielles.

Nous sommes passés d'un Internet libertaire à un **Internet sous double tutelle** :

- celle des entreprises qui vous traquent pour mieux vous vendre ;
- celle des États qui vous surveillent (parfois pour de bonnes raisons, souvent sans contrôle).

Face à cela, l'individu seul se sent impuissant. « De toute façon, ils ont déjà toutes mes données. » « Je ne peux rien y changer. » C'est ce qu'on appelle **l'éloge de l'apathie** – et c'est l'arme la plus efficace des Big Tech et des gouvernements autoritaires.

Une alternative existe : reprendre le contrôle

Sauf que... c'est faux. On peut résister. On peut reprendre le contrôle, un outil à la fois, un service à la fois.

Pas besoin de changer du jour au lendemain. Pas besoin de tout auto-héberger ou de disparaître du réseau. L'objectif n'est pas la perfection ; c'est **la progression**.

Chaque fois que vous remplacez Gmail par Proton Mail, WhatsApp par SimpleX ou Element, Google Maps par Organic Maps, Google Drive par Cryptpad ou Syncthing, vous retirez une petite brique à l'édifice de la surveillance et de la marchandisation. Vous devenez un peu plus propriétaire de votre vie numérique.

Ces fiches pratiques sont exactement cela : **une boîte à outils d'autodéfense numérique**.

Elles ne partent pas du principe que vous êtes un expert. Elles partent de vos usages quotidiens : le navigateur, les mots de passe, le cloud, la messagerie, le smartphone, l'ordinateur, le routeur, la box... et elles vous montrent, étape par étape, comment remplacer les services prédateurs par des alternatives libres, éthiques, décentralisées, ou au minimum respectueuses de votre vie privée.

Ce que vous allez trouver dans ce guide

- **Des solutions concrètes** pour chaque besoin (mail, cloud, cartographie, réseau social, mots de passe, 2FA, sauvegardes...).
- **Des comparaisons claires** entre les grandes options (Bitwarden / KeePass / Proton Pass, Organic Maps / Magic Earth, etc.).
- **Des mises en garde** sur les pièges courants (Google Authenticator, Cloud Act, UPnP, WPS, liens trackés...).
- **Des challenges** pour tester et adopter durablement de nouveaux réflexes.
- **Une philosophie** : pas de culte de la pureté, pas de paranoïa, mais une stratégie de reprise de contrôle progressive et réaliste.

Ce que vous ne trouverez pas (et pourquoi)

Ce guide n'est pas un manifeste contre le progrès ou une incitation à la clandestinité numérique. Il ne vous demande pas de devenir un hacker ou de vivre hors réseau. Il vous donne simplement les moyens de **choisir** : choisir qui voit vos données, choisir de ne pas être le produit, choisir de ne pas être surveillé sans raison.

Dernier conseil avant de commencer

N'ouvrez pas toutes ces fiches en même temps. Prenez une fiche, une seule, celle qui correspond à votre besoin le plus immédiat. Installez l'alternative. Laissez-vous le temps de vous habituer. Puis passez à la suivante.

C'est ainsi que l'on reprend le contrôle : **pas à pas, victoire après victoire.**

L'apathie dit : « C'est trop tard, trop compliqué, trop tard. »

Ces fiches disent : « **Commence aujourd'hui. Même petit. Ici et maintenant.** »

Bonne lecture, et bienvenue dans votre souveraineté numérique.