GUIDE DE SOUVERAINETÉ NUMÉRIQUE

Fiches pratiques pour reprendre le contrôle de votre vie numérique

Débutants & utilisateurs avancés



Méthode d'émancipation numérique en 4 vagues

Gabriel Ananda gabriel.ananda@mailo.com

Version 5.1

11 novembre 2026

CC BY SA

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.

gabriel.ananda@mailo.com
CC BY SA

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.

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 Session ou Element, Google Maps par Organic Maps ou Magic Earth, 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.

📌 Comment utiliser ce guide : la méthode des vagues successives

Vous venez de lire l'histoire de notre liberté numérique : comment nous sommes passés d'un Internet ouvert et décentralisé à un univers de surveillance et de marchandisation. Et vous vous dites peut-être : "C'est bien beau, mais par où commencer ?"

La réponse est simple : **pas à pas, vague après vague.**

Ce guide contient 89 fiches pratiques. Si vous les lisez toutes d'un seul coup, vous risquez la **surcharge cognitive** : trop d'informations, trop d'actions à mener, trop de décisions à prendre. Le risque ? Vous décourager et ne rien faire.

Pour éviter cela, nous vous proposons une **approche par vagues successives**. L'idée est simple : vous ne devez pas tout faire en même temps. Vous allez avancer **par étapes**, en consolidant chaque nouvelle habitude avant de passer à la suivante.

gabriel.ananda@mailo.com

🌊 Les 4 vagues pour une transition progressive, précédées d'une Vague 0.

La Vague 0 est un pré-requis, spécialement pour les débutants.

Vague	Objectif	Fiches concernées
Vague 0	**Comprendre le vocabulaire** (1 semaine)	Petit guide pour comprendre l'informatique sans se prendre la tête
Vague 1	**Les bases de la sécurité** (2 semaines)	N°16 (mots de passe), N°18 (2FA), N°2 (navigateur), N°17 (moteur de recherche), N°52 (téléphone)
Vague 2	**Protéger ses communications** (3 semaines)	N°10 (email éthique), N°15 (messagerie instantanée), N°6 (DNS), N°56 (alias de courriel), N°65 (clés d'accès)
Vague 3	**Libérer ses données** (1 mois)	N°7 (cloud), N°3 (YouTube), N°21 (RSS), N°24 (cartographie), N°50 (récupérer ses données), N°55 (photos), N°59 (agenda et contacts)
Vague 4	**Aller plus loin** (selon vos besoins)	N°13a et N°13b (Linux), N°20 (auto-hébergement), N°38 (Pi-hole), N°27 (Tor), N°44 (limites du VPN), N°64 (téléphone sans Google), N°68 (SMS chiffrés)

💡 Comment lire ce guide

1. **Ne sautez pas les vagues** : Chaque vague prépare la suivante. Par exemple, sans gestionnaire de mots de passe (Vague 1), activer la 2FA (Vague 1) ou changer de messagerie (Vague 2) est plus complexe.
2. **Prenez votre temps** : Une vague peut durer plusieurs semaines. L'objectif est d'intégrer durablement les nouvelles habitudes, pas de cocher des cases.
3. **Une fiche à la fois** : Ne lisez pas toutes les fiches d'une vague en même temps. Prenez une fiche, appliquez-la, testez-la, puis passez à la suivante.
4. **Adaptez à votre rythme** : Si une fiche vous semble trop technique, passez à la suivante et revenez-y plus tard. L'important est de progresser, pas d'être parfait.

gabriel.ananda@mailo.com

🎯 Pourquoi cette méthode fonctionne

•**Diminue l'anxiété** : Vous ne vous sentez pas submergé par une montagne de choses à faire.
•**Renforce la confiance** : Chaque petite victoire (changer de navigateur, sécuriser ses mots de passe) vous motive à continuer.
•**Évite les erreurs** : En allant trop vite, on fait des impasses (ex: oublier la 2FA après avoir changé de gestionnaire de mots de passe). Les vagues vous protègent de ces oublis.

📋 Votre plan d'action personnel

1.**Commencez par la Vague 1**. Ouvrez la fiche N°16, installez un gestionnaire de mots de passe, changez vos mots de passe importants. Prenez une semaine pour vous habituer.
2.**Passez à la Vague 2**. Une fois les bases en place, protégez vos communications : messagerie éthique, messagerie instantanée, DNS et alias de courriel.
3.**Continuez à votre rythme**. Les vagues 3 et 4 vous attendent quand vous serez prêt.
Lorsque vous aurez terminé les 3 premières vagues, vous aurez déjà fait l'essentiel du chemin vers votre souveraineté numérique.
Pour les autres fiches, prenez votre temps et voyez ce qui vous parle en fonction de vos besoins propres.

Rappel : L'objectif n'est pas la perfection, c'est la progression. Chaque petit pas vous rapproche de votre souveraineté numérique.

Table des matières

Chaque titre ci-dessous est un lien : il ouvre la fiche depuis le site guide.gabriel-ananda.org, qui vous redirige vers le fichier dans le dossier partagé sur Proton Drive. Une connexion Internet est donc nécessaire. Les liens fonctionnent de la même façon sous Windows, macOS, Linux, sur ordinateur comme sur téléphone. Ce site n'utilise ni

cookie ni traceur : il compte seulement, de façon anonyme, le nombre de téléchargements de chaque fiche.

Introduction

⇒ Petit guide pour comprendre l'informatique sans se prendre la tête :
Glossaire de 36 notions de base, avec analogies simples (maison, voiture, océan, restaurant). **À lire en premier si vous débutez.**
•**Partie 1 :** Les bases (ordinateur, OS, logiciel, Internet/Web, navigateur, moteur de recherche, logiciel propriétaire/libre, pièges des « gratuits »)
•**Partie 2 :** Notions complémentaires (cloud, chiffrement, donnée, IP, pare-feu, cookie, VPN, serveur, client, protocole, permissions, base de données, mot de passe, DNS, sauvegarde, antivirus, intelligence artificielle, hameçonnage, objets connectés, alias de courriel, fuite de données, NFC, OpenPGP, Fédivers, mise à jour, format ouvert et DRM)
•**Partie 3 :** Récapitulatif général (tableau des 36 notions, phrase à retenir, trois conseils pour commencer)

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

Fiche N°1 : Libérez-vous des suites bureautiques propriétaires
Fiche N°23 : Éditez vos photos sans Lightroom – GIMP, darktable et RawTherapee, alternatives libres à la suite Adobe
Fiche N°71 : Faites des visioconférences sans Zoom ni Teams
Fiche N°74 : Traduisez sans Google Traduction

🌐 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 – Supprimez les traceurs dans les URL
Fiche N°14b : Pour aller plus loin – Tous les cas particuliers du nettoyage de liens
Fiche N°41 : Raccourcissez vos URLs en souveraineté numérique

🔍 Moteurs de recherche (remplacer Google Search, Bing)

Fiche N°17 : Remplacez Google par un moteur de recherche qui ne vous traque pas

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

Fiche N°10 : Quittez Gmail, Outlook et Yahoo pour un mail éthique
Fiche N°36 : Auto-hébergement mail pur – Installez votre propre serveur e-mail avec mailcow, Mailu ou Maddy
Fiche N°56 : Protégez votre adresse e-mail avec des alias

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

Fiche N°15 : Remplacez WhatsApp, Messenger et Telegram par Element, SimpleX ou Session – Des messageries sans numéro de téléphone et sans pistage
Fiche N°33 : Element et Matrix, guide détaillé – La messagerie décentralisée pour remplacer WhatsApp, Slack et Telegram
Fiche N°49 : Communiquez sans Internet avec Meshtastic (ou Bitchat)
Fiche N°68 : Chiffrez vos SMS avec foomms et foodjis

☁️ **Cloud, stockage et synchronisation (remplacer Google Drive, iCloud, OneDrive, Dropbox, WeTransfer, Google Keep)**

Fiche N°7 : Trouvez une alternative libre à Google Drive et Google Doc
Fiche N°29 : Synchronisez vos appareils sans cloud avec Syncthing – Adieu Google Drive, OneDrive et iCloud
Fiche N°31 : Utilisez un NAS pour centraliser et sauvegarder vos données – Complément aux sauvegardes locales
Fiche N°34 : Nextcloud, auto-hébergement pas à pas – Votre cloud privé pour remplacer Google Drive, iCloud et OneDrive
Fiche N°55 : Libérez vos photos de Google Photos et iCloud
Fiche N°59 : Synchronisez agenda et contacts sans Google
Fiche N°72 : Envoyez de gros fichiers sans WeTransfer
Fiche N°73 : Prenez vos notes sans Google Keep ni Evernote

Téléphones et alternatives mobiles (remplacer Play Store, services Google)

Fiche N°42 : Aurora Store – Google Play Store sans compte Google
Fiche N°52 : Réglez la confidentialité de votre téléphone
Fiche N°57 : Changez le clavier de votre téléphone
Fiche N°64 : Passez à un téléphone sans Google

🔐 Sécurité, mots de passe et chiffrement

Fiche N°16 : Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass, libres et sans Big Tech
Fiche N°18 : Activez l'authentification à deux facteurs (2FA)
Fiche N°26 : Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol
Fiche N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous
Fiche N°37 : Vérifiez l'intégrité des fichiers avec GPG – Signatures et sommes de contrôle
Fiche N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur
Fiche N°65 : Passez aux clés d'accès (passkeys)

🗺️ Cartographie (remplacer Google Maps, Waze, Apple Plans)

Fiche N°24 : Remplacez Google Maps par Organic Maps, Magic Earth, OpenStreetMap, IGN ou Visorando – Naviguez sans être pisté

🎬 Vidéo, musique, livres et streaming (remplacer YouTube, Spotify, Kindle)

Fiche N°3 : Regardez YouTube sans publicités
Fiche N°25 : Auto-hébergez une instance PeerTube – Publiez des vidéos sans YouTube
Fiche N°43 : Installez votre propre instance PeerTube – Hébergez vos vidéos sans publicité ni censure
Fiche N°54 : Regardez YouTube sans publicité sur votre Google TV
Fiche N°62 : Écoutez musique et podcasts sans Spotify
Fiche N°75 : Lisez des livres numériques sans Amazon Kindle

🛡️ 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°45 : Installez et utilisez Warren VPN (bêta gratuite, version payante à venir)
Fiche N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité
Fiche N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau
Fiche N°38 : Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau
Fiche N°44 : Les limites du VPN – L'anonymat réel et le brouillage d'empreinte
Fiche N°60 : Réglez vos objets connectés

🗑️ Désintoxication numérique (quitter les big tech)

Fiche N°9 : Désactivez les fonctions cloud des Big Tech
Fiche N°12 : Renoncez progressivement aux services des Big Tech
Fiche N°13a : Passez à Linux – Préparez l'installation et testez Linux Mint
Fiche N°13b : Passez à Linux – Installez Linux Mint et faites vos premiers pas
Fiche N°78 : Installez vos logiciels et faites vos mises à jour sous Linux Mint
Fiche N°39 : Nettoyez votre empreinte numérique – Supprimez vos comptes inutilisés, réduisez votre exposition et exercez vos droits RGPD
Fiche N°50 : Récupérez vos données stockées chez les GAFAM

📝 Sondages et formulaires (remplacer Google Forms, Doodle)

Fiche N°8 : Trouvez une alternative libre à Doodle

🏠 Auto-hébergement et serveurs personnels

Fiche N°20 : Auto-hébergez vos services avec YunoHost – Devenez votre propre cloud
Fiche N°20a : Configurer WireGuard sur YunoHost pour un accès VPN sécurisé
Fiche N°20b : Installer et configurer SearXNG sur un sous-domaine local avec YunoHost
Fiche N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost
Fiche N°20d : Installer et configurer Jitsi Meet sur un VPS avec YunoHost
Fiche N°20e : Installer et configurer PeerTube sur un VPS avec YunoHost
Fiche N°28 : Choisissez un hébergeur web européen et éthique – Reprenez le contrôle de vos sites et données

🧅 Anonymat et sécurité extrême

Fiche N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion
Fiche N°32 : Installez et utilisez Tails – Naviguez anonymement sans laisser de traces

💾 Sauvegardes (remplacer iCloud Backup, Google Backup)

Fiche N°19a : Sauvegardez vos données localement sous Linux Mint
Fiche N°19b : Sauvegardez vos données localement sous Windows
Fiche N°19c : Sauvegardez vos données localement sous macOS
Fiche N°19d : Sauvegardez vos données localement sous Android
Fiche N°19e : Sauvegardez vos données localement sur iPhone (iOS)

📰 **Agrégateur RSS (remplacer les réseaux sociaux et newsletters)**
Fiche N°21 : Utilisez un agrégateur RSS (FreshRSS, Feedly) – Reprenez le contrôle de votre fil d'actualités

🐘 **Réseaux sociaux (remplacer Twitter, Facebook, Instagram)**
Fiche N°22 : Remplacez Twitter par Mastodon ou Bluesky – Rejoignez le Fédiverse sans algorithme ni publicité
Fiche N°76 : Quittez Facebook et Instagram

🤖 **Intelligence artificielle (IA locale et assistants européens d'abord, sans livrer sa vie privée)**
Fiche N°53 : Utilisez l'IA sans livrer votre vie privée

Conseils pratiques à mettre en œuvre sans aucune installation supplémentaire
Fiche N°46 : Les 20 gestes de base sans outil
Fiche N°47 : Reconnaître et déjouer les arnaques en ligne
Fiche N°48 : 14 outils de cybersécurité dans votre navigateur
Fiche N°51 : Préparez votre héritage numérique
Fiche N°58 : Réagissez à une fuite de données
Fiche N°61 : Protégez vos enfants en ligne sans les espionner
Fiche N°63 : Payez en préservant votre vie privée
Fiche N°66 : Stoppez le démarchage téléphonique
Fiche N°67 : Accompagnez un proche débutant
Fiche N°69 : Récupérez un compte piraté
Fiche N°70 : Sécurisez vos démarches administratives en ligne
Fiche N°77 : Faites durer vos appareils

Dans le même répertoire vous trouverez aussi un fichier de suivi de votre progression :
Suivez votre progression sans compte

CC BY SA

🔁 Classement par niveau de difficulté

Niveau	N° des fiches
★☆☆☆☆ (Très facile)	N°1, N°2, N°3 (selon la méthode), N°8, N°14a, N°17, N°46, N°47, N°48, N°51, N°52, N°53, N°56, N°57, N°58, N°63, N°66, N°70, N°71, N°72, N°74, N°77
★★☆☆☆ (Facile)	N°4, N°5, N°6, N°7, N°9, N°10, N°12, N°13a, N°13b, N°15, N°16, N°18, N°19a-e, N°21, N°22, N°24, N°26, N°27, N°29, N°30, N°33, N°39, N°41, N°42, N°45, N°49, N°50, N°54, N°55, N°59, N°60, N°61, N°62, N°65, N°67, N°69, N°73, N°75, N°76, N°78
★★★☆☆ (Moyen)	N°11, N°14b, N°20, N°20a à N°20e, N°23, N°25 (Facile en rejoignant une instance), N°28, N°31, N°32, N°34 (Facile avec YunoHost), N°35, N°37, N°38, N°40, N°43, N°44, N°68
★★★★☆ (Avancé)	N°36, N°64

gabriel.ananda@mailo.com

📈 Suggestions de lecture par profil

Vous êtes…	Commencez par les fiches…
Débutant	Petit Guide → N°1 (bureautique) → N°2 (navigateur) → N°3 (YouTube) → N°10 (email) → N°16 (mots de passe) → N°41 (liens courts) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°52 (téléphone) → N°53 (IA) → N°56 (alias) → N°57 (clavier) → N°58 (fuite de données) → N°66 (démarchage) → N°69 (compte piraté) → N°70 (démarches en ligne) → N°74 (traduction)
Famille / particulier	Petit Guide → N°10 (email) → N°15 (messagerie) → N°24 (cartographie) → N°31 (NAS) → N°41 (liens courts) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°50 (récupérer ses données) → N°51 (héritage numérique) → N°52 (téléphone) → N°54 (YouTube sur Google TV) → N°55 (photos) → N°60 (objets connectés) → N°61 (enfants) → N°63 (paiement) → N°65 (clés d'accès) → N°66 (démarchage) → N°67 (accompagner un proche) → N°71 (visio) → N°72 (gros fichiers) → N°75 (livres numériques) → N°77 (faire durer ses appareils)
Entreprise / association	Petit Guide → N°20 (Yunohost) → N°28 (hébergeur) → N°25 (Peertube) → N°43 (PeerTube sur VPS) → N°33 (Matrix) → N°40 (BIOS/UEFI) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°53 (IA) → N°59 (agenda et contacts) → N°71 (visio) → N°72 (gros fichiers) → N°73 (notes)
Militant / journaliste	Petit Guide → N°44 (limites du VPN) → N°27 (Tor) → N°32 (Tails) → N°15 (SimpleX) → N°18 (2FA) → N°39 (empreinte numérique) → N°40 (BIOS/UEFI) → N°49 (Meshtastic) → N°52 (téléphone) → N°53 (IA) → N°57 (clavier) → N°64 (téléphone sans Google) → N°68 (SMS chiffrés)
Exigeant / paranoïaque	Petit Guide → N°5 (Mullvad) → N°36 (mail pur) → N°37 (GPG) → N°38 (Pi-hole) → N°35 (Vaultwarden) → N°40 (BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°49 (Meshtastic) → N°53 (IA locale) → N°64 (téléphone sans Google) → N°68 (SMS chiffrés)
Curieux de Linux	N°13a et N°13b (Linux) → N°20 (Yunohost) → N°34 (Nextcloud) → N°40

gabriel.ananda@mailo.com
CC BY SA

Vous êtes…	Commencez par les fiches…
	(BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°53 (IA locale) → N°55 (Immich) → N°62 (Navidrome) → N°64 (téléphone sans Google) → N°77 (faire durer ses appareils) → N°78 (logiciels sous Linux Mint)
Anonymat renforcé	Petit Guide → N°44 (limites du VPN) → N°5 (Mullvad) → N°27 (Tor) → N°32 (Tails) → N°36 (mail pur) → N°40 (BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité) → N°49 (Meshtastic) → N°63 (paiement) → N°64 (téléphone sans Google) → N°45 (Warren VPN, en test)

gabriel.ananda@mailo.com

Ce que vous allez trouver dans ce guide

•Un glossaire (**petit guide pour comprendre l'informatique sans se prendre la tête**) à destination des débutants.
•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. »
L'important ce n'est pas la perfection, c'est la progression !

Bonne lecture, et bienvenue dans votre souveraineté numérique.

gabriel.ananda@mailo.com

Annexe : Liens croisés entre les 36 notions du glossaire et les fiches du Guide de Souveraineté Numérique

---

Partie 1 : Les bases de l'informatique

Notion du glossaire	Fiche(s) associée(s) du guide	Pourquoi ce lien
§1 – Ordinateur / PC	N°13a et N°13b – Passez à Linux (préparer, puis installer) N°40 – Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur N°77 – Faites durer vos appareils	Les fiches N°13a et N°13b aident à choisir un système d'exploitation ; la N°40 protège la première porte d'entrée matérielle de l'ordinateur
§2 – Système d'exploitation (OS)	N°13a et N°13b – Passez à Linux (préparer, puis installer) N°19a – Sauvegardez vos données localement sous Linux Mint N°19b – Sauvegardez vos données localement sous Windows N°19c – Sauvegardez vos données localement sous macOS N°64 – Passez à un téléphone sans Google N°78 – Installez vos logiciels et faites vos mises à jour sous Linux Mint	Chaque fiche de sauvegarde est spécifique à un OS

gabriel.ananda@mailo.com

§3 – Logiciel / Application	Toutes les fiches	Chaque fiche recommande des logiciels alternatifs
§4 – Internet vs Web	N°2 – Naviguez sans être pisté (protection de base) N°17 – Remplacez Google par un moteur de recherche qui ne vous traque pas	Distinction fondamentale pour comprendre le navigateur et le moteur de recherche
§5 – Navigateur web	N°2 – Naviguez sans être pisté (protection de base) N°11 – Naviguez sans être pisté (protection avancée) N°14a – Nettoyez vos liens partagés – Supprimez les traceurs dans les URL N°14b – Pour aller plus loin – Tous les cas particuliers du nettoyage de liens N°41 – Raccourcissez vos URLs en souveraineté numérique	Toutes les fiches liées à la navigation web
§6 – Moteur de recherche	N°17 – Remplacez Google par un moteur de recherche qui ne vous traque pas N°20b – Installer et configurer SearXNG sur un sous-domaine local avec YunoHost	SearXNG est un métamoteur auto-hébergé
§7 – Logiciel propriétaire	N°1 – Libérez-vous des suites bureautiques propriétaires N°23 – Éditez vos photos sans Lightroom – GIMP, darktable et RawTherapee, alternatives libres à la suite Adobe N°13a et N°13b – Passez à Linux (préparer, puis installer)	Alternatives aux logiciels propriétaires
§8 – Logiciel libre /	N°1 – Libérez-vous des suites	Toutes les alternatives libres

gabriel.ananda@mailo.com

Open Source	bureautiques propriétaires N°23 – Éditez vos photos sans Lightroom – GIMP, darktable et RawTherapee, alternatives libres à la suite Adobe N°20 – Auto-hébergez vos services avec YunoHost – Devenez votre propre cloud	recommandées
§9 – Les pièges des « gratuits » en ligne	N°10 – Quittez Gmail, Outlook et Yahoo pour un mail éthique N°12 – Renoncez progressivement aux services des Big Tech N°22 – Remplacez Twitter par Mastodon ou Bluesky – Rejoignez le Fédiverse sans algorithme ni publicité N°76 – Quittez Facebook et Instagram	Comprendre pourquoi Gmail, Facebook, etc. sont problématiques
§10 – Récap des bases	—	Synthèse, pas de fiche associée

Partie 2 : Notions complémentaires

Notion du glossaire	Fiche(s) associée(s) du guide	Pourquoi ce lien
§11 – Cloud	N°7 – Trouvez une alternative libre à Google Drive et Google Doc N°29 – Synchronisez vos appareils sans cloud avec Syncthing – Adieu Google Drive, OneDrive et iCloud N°31 – Utilisez un NAS pour centraliser et sauvegarder vos données	Toutes les alternatives au cloud propriétaire

gabriel.ananda@mailo.com

	– Complément aux sauvegardes locales N°34 – Nextcloud, auto-hébergement pas à pas – Votre cloud privé pour remplacer Google Drive, iCloud et OneDrive N°55 – Libérez vos photos de Google Photos et iCloud N°59 – Synchronisez agenda et contacts sans Google N°72 – Envoyez de gros fichiers sans WeTransfer N°73 – Prenez vos notes sans Google Keep ni Evernote	
§12 – Chiffrement	N°26 – Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol N°37 – Vérifiez l'intégrité des fichiers avec GPG – Signatures et sommes de contrôle N°18 – Activez l'authentification à deux facteurs (2FA) N°10 – Quittez Gmail, Outlook et Yahoo pour un mail éthique N°15 – Remplacez WhatsApp, Messenger et Telegram par Element, SimpleX ou Session – Des messageries sans numéro de téléphone et sans pistage N°73 – Prenez vos notes sans Google Keep ni Evernote	Chiffrement des fichiers, des emails, des messageries
§13 – Donnée	N°39 – Nettoyez votre empreinte numérique – Supprimez vos comptes inutilisés, réduisez votre exposition et exercez vos droits RGPD	Comprendre ce que les Big Tech collectent

gabriel.ananda@mailo.com

	N°9 – Désactivez les fonctions cloud des Big Tech N°50 – Récupérez vos données stockées chez les GAFAM N°53 – Utilisez l'IA sans livrer votre vie privée N°58 – Réagissez à une fuite de données N°63 – Payez en préservant votre vie privée N°66 – Stoppez le démarchage téléphonique N°76 – Quittez Facebook et Instagram	
§14 – Adresse IP	N°4 – Installez et utilisez Proton VPN (version gratuite possible) N°5 – Installez et utilisez Mullvad VPN (version payante uniquement) N°45 – Installez et utilisez Warren VPN (bêta gratuite, version payante à venir) N°44 – Les limites du VPN – L'anonymat réel et le brouillage d'empreinte	Les VPN masquent l'adresse IP
§15 – Pare-feu	N°30 – Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau N°38 – Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau N°60 – Réglez vos objets connectés	Protection réseau et blocage des publicités
§16 – Cookie	N°2 – Naviguez sans être pisté (protection de base) N°11 – Naviguez sans être pisté (protection avancée)	Gestion des cookies et des traqueurs
§17 – VPN	N°4 – Installez et utilisez Proton VPN	Toutes les fiches VPN

gabriel.ananda@mailo.com
CC BY SA

	(version gratuite possible) N°5 – Installez et utilisez Mullvad VPN (version payante uniquement) N°45 – Installez et utilisez Warren VPN (bêta gratuite, version payante à venir) N°44 – Les limites du VPN – L'anonymat réel et le brouillage d'empreinte N°20a – Configurer WireGuard sur YunoHost pour un accès VPN sécurisé	
§18 – Serveur	N°20 – Auto-hébergez vos services avec YunoHost – Devenez votre propre cloud N°28 – Choisissez un hébergeur web européen et éthique – Reprenez le contrôle de vos sites et données N°31 – Utilisez un NAS pour centraliser et sauvegarder vos données – Complément aux sauvegardes locales N°34 – Nextcloud, auto-hébergement pas à pas – Votre cloud privé pour remplacer Google Drive, iCloud et OneDrive N°43 – Installez votre propre instance PeerTube – Hébergez vos vidéos sans publicité ni censure	Auto-hébergement et serveurs personnels
§19 – Client	N°4 – Installez et utilisez Proton VPN (version gratuite possible) N°5 – Installez et utilisez Mullvad VPN (version payante uniquement) N°45 – Installez et utilisez Warren VPN (bêta gratuite, version payante à venir)	Les applications VPN sont des clients
§20 – Protocole	N°6 – Changez votre serveur DNS	DNS, WireGuard, CalDAV et

gabriel.ananda@mailo.com

	pour plus de confidentialité et de sécurité N°20a – Configurer WireGuard sur YunoHost pour un accès VPN sécurisé N°59 – Synchronisez agenda et contacts sans Google	CardDAV sont des protocoles
§21 – Permissions	N°40 – Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur N°52 – Réglez la confidentialité de votre téléphone N°57 – Changez le clavier de votre téléphone N°61 – Protégez vos enfants en ligne sans les espionner	Gestion des droits d'accès au matériel et des autorisations des applications
§22 – Base de données	N°34 – Nextcloud, auto-hébergement pas à pas – Votre cloud privé pour remplacer Google Drive, iCloud et OneDrive	Nextcloud utilise une base de données
§23 – Mot de passe / authentification	N°16 – Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass, libres et sans Big Tech N°18 – Activez l'authentification à deux facteurs (2FA) N°35 – Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous N°51 – Préparez votre héritage numérique N°56 – Protégez votre adresse e-mail avec des alias N°58 – Réagissez à une fuite de données N°65 – Passez aux clés d'accès (passkeys)	Gestion des mots de passe et 2FA

gabriel.ananda@mailo.com

	N°69 – Récupérez un compte piraté	
§24 – DNS	N°6 – Changez votre serveur DNS pour plus de confidentialité et de sécurité N°20b – Installer et configurer SearXNG sur un sous-domaine local avec YunoHost N°20c – Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost	DNS et services associés
§25 – Sauvegarde	N°19a – Sauvegardez vos données localement sous Linux Mint N°19b – Sauvegardez vos données localement sous Windows N°19c – Sauvegardez vos données localement sous macOS N°19d – Sauvegardez vos données localement sous Android N°31 – Utilisez un NAS pour centraliser et sauvegarder vos données – Complément aux sauvegardes locales N°50 – Récupérez vos données stockées chez les GAFAM N°51 – Préparez votre héritage numérique	Toutes les fiches de sauvegarde
§26 – Antivirus / malware	N°38 – Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau N°26 – Chiffrez vos fichiers sensibles avec Cryptomator ou VeraCrypt – Protégez vos données même en cas de vol	Blocage des malwares et protection des données
§27 – Intelligence artificielle	N°53 – Utilisez l’IA sans livrer votre vie privée	Assistants d'IA, réglages et IA locale

gabriel.ananda@mailo.com

§28 – Hameçonnage	N°47 – Reconnaître et déjouer les arnaques en ligne N°58 – Réagissez à une fuite de données N°56 – Protégez votre adresse e-mail avec des alias N°69 – Récupérez un compte piraté N°70 – Sécurisez vos démarches administratives en ligne	Repérer les faux messages et limiter leur portée
§29 – Objets connectés	N°60 – Réglez vos objets connectés N°54 – Regardez YouTube sans publicité sur votre Google TV N°38 – Installez Pi-hole – Bloquez les publicités et les traqueurs au niveau de votre réseau	Téléviseur, assistant vocal, caméras, réseau domestique
§30 – Alias de courriel	N°56 – Protégez votre adresse e-mail avec des alias N°10 – Quittez Gmail, Outlook et Yahoo pour un mail éthique	Une adresse par site, en plus de la messagerie principale
§31 – Fuite de données	N°58 – Réagissez à une fuite de données N°16 – Gérez vos mots de passe avec Bitwarden, KeePass ou Proton Pass, libres et sans Big Tech N°18 – Activez l'authentification à deux facteurs (2FA)	Que faire quand ses données ont fuité, et comment limiter les dégâts
§32 – NFC (sans contact)	N°68 – Chiffrez vos SMS avec foomms et foodjis N°65 – Passez aux clés d'accès (passkeys)	Présenter une clé de sécurité au dos du téléphone
§33 – OpenPGP	N°68 – Chiffrez vos SMS avec foomms et foodjis N°37 – Vérifiez l'intégrité des fichiers avec GPG – Signatures et sommes de contrôle	Chiffrer et signer avec une clé publique et une clé privée

gabriel.ananda@mailo.com

§34 – Fédivers	N°22 – Remplacez Twitter par Mastodon ou Bluesky – Rejoignez le Fédiverse sans algorithme ni publicité N°76 – Quittez Facebook et Instagram N°25 – Auto-hébergez une instance PeerTube – Publiez des vidéos sans YouTube N°71 – Faites des visioconférences sans Zoom ni Teams N°72 – Envoyez de gros fichiers sans WeTransfer	Mastodon, Pixelfed, PeerTube, Mobilizon ; choisir une instance (Jitsi, Lufi)
§35 – Mise à jour	N°13a – Passez à Linux – Préparez l’installation et testez Linux Mint N°78 – Installez vos logiciels et faites vos mises à jour sous Linux Mint N°77 – Faites durer vos appareils N°64 – Passez à un téléphone sans Google N°30 – Mettez à jour votre box et votre routeur – Sécurisez la porte d’entrée de votre réseau	Correctifs de sécurité, fin de support de Windows 10 et des vieux téléphones
§36 – Format ouvert et DRM	N°75 – Lisez des livres numériques sans Amazon Kindle N°73 – Prenez vos notes sans Google Keep ni Evernote N°1 – Libérez-vous des suites bureautiques propriétaires N°50 – Récupérez vos données stockées chez les GAFAM N°76 – Quittez Facebook et Instagram	Des fichiers lisibles partout, et des données qu'on peut emporter

gabriel.ananda@mailo.com

Tableau récapitulatif synthétique

#	Notion	Fiches principales
1	Ordinateur / PC	N°13a-b, N°40, N°77
2	Système d'exploitation	N°13a-b, N°19a-d, N°64, N°78
3	Logiciel / Application	Toutes
4	Internet vs Web	N°2, N°17
5	Navigateur web	N°2, N°11, N°14a, N°14b, N°41
6	Moteur de recherche	N°17, N°20b
7	Logiciel propriétaire	N°1, N°23, N°13
8	Logiciel libre / Open Source	N°1, N°23, N°20
9	Pièges des « gratuits »	N°10, N°12, N°22, N°76
10	Récap des bases	—
11	Cloud	N°7, N°29, N°31, N°34, N°55, N°59, N°72, N°73
12	Chiffrement	N°26, N°37, N°18, N°10, N°15, N°73
13	Donnée	N°39, N°9, N°50, N°53, N°58, N°63, N°66, N°76
14	Adresse IP	N°4, N°5, N°45, N°44
15	Pare-feu	N°30, N°38, N°60
16	Cookie	N°2, N°11
17	VPN	N°4, N°5, N°45, N°44, N°20a
18	Serveur	N°20, N°28, N°31, N°34, N°43
19	Client	N°4, N°5, N°45
20	Protocole	N°6, N°20a, N°59
21	Permissions	N°40, N°52, N°57, N°61
22	Base de données	N°34
23	Mot de passe / authentification	N°16, N°18, N°35, N°51, N°56,

gabriel.ananda@mailo.com

		N°58, N°65, N°69
24	DNS	N°6, N°20b, N°20c
25	Sauvegarde	N°19a-d, N°31, N°50, N°51
26	Antivirus / malware	N°38, N°26
27	Intelligence artificielle	N°53
28	Hameçonnage	N°47, N°58, N°56, N°69, N°70
29	Objets connectés	N°60, N°54, N°38
30	Alias de courriel	N°56, N°10
31	Fuite de données	N°58, N°16, N°18
32	NFC (sans contact)	N°68, N°65
33	OpenPGP	N°68, N°37
34	Fédivers	N°22, N°76, N°25, N°71, N°72
35	Mise à jour	N°13a, N°78, N°77, N°64, N°30
36	Format ouvert et DRM	N°75, N°73, N°1, N°50, N°76

Comment utiliser ces liens croisés

1.**Pour les débutants :** Lisez d'abord le glossaire (§1 à §36), puis ouvrez les fiches associées une par une.
2.**Pour les utilisateurs avancés :** Utilisez les fiches comme point d'entrée, et consultez le glossaire pour les notions que vous ne maîtrisez pas.
3.**Pour les formateurs :** Ces liens permettent de construire des parcours pédagogiques cohérents (ex. : « Comprendre le VPN » = §17 + N°4 + N°5 + N°45 + N°44).

gabriel.ananda@mailo.com
CC BY SA