Protéger sa sphère privée numérique

Guide pratique vous permettant d'adapter votre attitude et de déployer des moyens pour protéger votre sphère privée

Edité par Spirwind – Version 1.02 – 2021
Contact : **spirwind@pm.me**

Table des matières

A. INTRODUCTION

GAFAM. Cet acronyme vous dit surement quelque chose? Il s'agit de Google, Apple, Facebook, Amazon, Microsoft. Entreprises mondiales du numérique. Vous savez également que toutes ces entreprises déploient des moyens humains et financiers considérables pour développer des produits, applications et plateformes en ligne qui vous seront dans une grande majorité des cas proposés gratuitement ! Connaissant leur avidité de plus en plus visible pour l'argent et le pouvoir, une question majeure et centrale est à poser : Pourquoi est-ce gratuit ? A l'origine, le business de ces entreprises reposait principalement dans la construction de réseaux publicitaires ciblés et à grande échelle leur permettant ainsi d'engranger des profits considérables.Et c'est toujours le cas. Mais aujourd'hui en plus, nous avons sans nul doute tous constaté que ces entreprises avaient récemment fait évoluer leur doctrine en s'immissant toujours plus dans les profondeurs de ce que révèle l'utilisation de notre smartphone. Le smartphone est leur support majeur ! Comprenez bien cela. Il y a biensur d'autres support tel que l'ordinateur, la tablette mais le téléphone est sans aucun doute leur favoris ! Pourquoi? Hey bien, disons que vous l'avez constamment dans votre poche ! Au quotidien, vous l'utilisez pour appeler, Qui? Pour chercher votre recette favorite Quoi? Envoyer un message instantané à votre mere Pourquoi ? Pour vous rendre chez votre radiologue grâce au GPS Ou? Qui? Quoi? Pourquoi? Où? Voila que votre smartphone se met à poser ces questions auxquelles vous répondez naturellement, en vivant votre vie. De (trop) nombreuses personne objectertont qu'elle n'ont rien à cacher. Affirmer cela n'est autre que de dire que la liberté d'expression n'est pas essentielle. Et c'est bien là le piège. Les GAFAM mènent la danse de nos vies à travers toutes ces plateformes, ces applications et grâce à votre téléphone. De manière insidieuse et détournée. Pour conclure mon introduction, je dirai que les GAFAM sont désormais en mesure de supplenter nos gouvernements et de modeler nos vies selon leur vision. Je n'exclu pas non plus que le smartphone est un outil qui rend bien des services (Peut être trop?), et que d'une certaine manière personne ne pourra s'en passer. C'est pourquoi je vous explique à travers ce document les points essentiels à mettre en place et le comportement à adopter au quotidien lorsque vous utilisez votre smartphone.

B. OBJECTIFS

L’objectif de ce document est de vous apporter un guide permettant de mieux protéger votre sphère privée numérique dans l’utilisation de votre Smartphone.

- Protéger votre sphère privée?

Le niveau de protection de votre sphère privée résulte d’une façon d’utiliser votre smartphone. Il est influencé principalement par les applications que vous utiliserez et par les moyens techniques et des bonnes pratiques mis en place pour le renforcer au quotidien.

C. UTILISER SOBREMENT SON SMARTPHONE

1. Acheter son smartphone Android

Evitez les smartphones chinois ou Koréens d’une manière générale. Mais dîtes vous bien que quelques soit le constructeur, les systèmes d’exploitations Android sont plus ou moins modifiés.Ces systèmes modifiés sont appelés “surcouches” car Android est ouvert à tous : développeurs, concepteurs et fabricants d'appareils. Ainsi, toujours plus de personnes peuvent expérimenter de nouvelle fonctionnalité sur le système qui sera installé sur le smartphone que vous acheterez. Il existe des moyens de modifier ce système android sur votre smartphone par exemple en installant vous même une surcouche android aussi appelée ROM telle que **MicroG** mais cela nécessite des aptitudes techniques avancées.

2. Sécuriser et contrôler sa connexion avec un VPN

Une hypothèse (Très probable) importante est à prendre en compte. Votre FAI (Fournisseur d’accès à internet) peut se comporter comme une entreprise des GAFAM et même **collaborer avec l’état**.

- Comment peut-il faire cela ?

Imaginons que vous avez souscris à un abonnement internet. La compagnie vous livre votre box gratuitement et même la carte SIM pour votre smartphone. Le tout sera raccordé et mis en service en moins de 30 minutes.

- Et maintenant ?

Vous allumez votre smartphone et effectuez votre premiere recherche sur internet. C’est simple et rapide.

- Mais que se passe t-il derriere tout cela ?

Votre connexion identifiée par votre adresse IP sur le web est associé à votre nom, prénom, adresse, date de naissance etc…

Votre recherche, qu'elle soit effectuée depuis votre téléphone,depuis votre PC ou tablette, en utilisant le Wifi, la 4G ou la voie câblée va interroger ce que l'on appel un serveur DNS (Domain Name Server) propre à votre fournisseur pour vous rediriger vers le résultat de votre recherche. Vous voyez où je veux en venir ? Oui **votre FAI** est à cet instant en mesure d'associer à votre connexion en plus des informations qu'il possède deja, au **détail de votre recherche** et le résultat que vous avez choisi de consulter.

- Qu'est ce qu'un VPN ?

VPN est l'abréviation de « virtual private network » (réseau privé virtuel) un service qui protège votre connexion Internet et votre confidentialité en ligne. Un VPN crée un tunnel chiffré pour vos données, protège votre identité en ligne, vous permet de cacher l'adresse IP attribuée par votre FAI. Vos recherches, les flux de données de vos applications transitent alors via votre tunnel VPN. Un serveur VPN possède également ses propres adresses DNS.

- Oui mais lequel ?

Afin d'éviter de simplement délocaliser l'espionnage et le stockage des donnéees vous concernant, il ne faut pas choisir n'importe quel VPN. Les 2 critères importants à prendre en compte pour choisir son VPN sont :

- Le non stockage des "log" de vos connexions. (Certain VPN le font !)
- Le siège social de la société proposant un VPN en dehors des pays partenaires de l'alliance des 14 yeux.

Basé à l'isthme du panama, le VPN "**NordVPN**" est un très bon candidat. Sa juridiction propre au pays qui accueil son siège et sa politique "no log" en font un très bon VPN.

L'autre alternative est **ProtonVPN**, basé en suisse avec son excellente politique de protection des données personnelles et la non journalisation de vos connexions en font également un VPN de premier choix pour le **continent Européen.**

C’est pourquoi je vais vous montrer comment installer et paramétrer votre téléphone pour que toutes vos données transitent en permanence via votre nouveau VPN “NORDVPN” ou “PROTONVPN”

- Créer un compte sur le site www.nordvpn.com ou https://protonvpn.com/fr/

➔ Si possible utilisez une adresse email chiffrée comme décris plus bas dans ce document.

- Téléchargez et installer l’application Nord VPN ou ProtonVPN depuis votre store d’applications favoris.

Attention Etapes importante !

Une fois l’application installée portez une attention particulière aux réglages qui suivent :

a. Après vous être connecté avec votre adresse mail et votre mot de passe rendez vous dans les paramètres de l’application.

b. Dans la rubrique “Connexion automatique” sélectionnez “toujours”. Ceci vous permettant d’être protégé quelque soit le type de connexion utilisée par votre smartphone.

c. Rendez vous dans les paramètres de votre téléphone, rubrique “VPN”

d. Activer le VPN “ NordVPN “ si cela n’est pas deja fait puis cochez “VPN permanent”

e. Activer le blocage des connexions sans VPN.

f. Lancer une connexion rapide depuis votre application NordVPN ou ProtonVPN

Ca y est vos flux de données sont protégés !

Note : Le VPN se désactivera lors de chaque redémarrage de votre téléphone. Vous vous renderai compte qu’il n’y a alors aucune connexion, il vous suffit de faire la manipulation décrite au point f.

3. Contrôler les applications installées

Dîtes vous toujours que ce sont principalement les applications intallées sur votre smartphone qui représentent le plus de danger pour la sécurité et la confidentialité de vos données.

Android permet le contrôle des autorisations d'utilisation des différentes fonctions de votre téléphone et ce pour chaque applications. Cela correspond au message survenu lorque vous lancez une première fois une application nouvellement installée. Les choix que vous faites ne sont pas gravés dans le marbre. A condition que vous sachiez comment y revenir.

Dans le menu paramètres de votre téléphone, rendez vous dans la rubrique "Applis" puis "autorisations". La page listera les différentes fonctions du téléphone et le nombre d'applications ayant l'accès.

IL vous suffira alors de sélectionner la fonction souhaitée pour y voir les applications autorisées et ainsi pouvoir révoquer l'autorisation pour une ou plusieurs applications particulières.

De mon point de vue les fonctions suivantes sont les plus critiques :

- Appareil photo
- Localisation
- Microphone
- SMS
- Téléphone

Pensez à **révoquer** les autorisations des applications qui ne vous sont pas ou **peu utiles** car certaines applications peuvent fonctionner en arrière plan.

D'une manière générale **désinstallez** toutes les applications qui ne vous **servent plus**. Cela améliorera votre niveau de sécurité numérique.

4. Maîtriser les comptes utilisateurs d'arrière plan

La plupart des téléphones sont livrés avec une ribambelle d'applications toutes l**iées a GOOGLE**. Il faut être conscient que lorsque vous en utiliserai une par exemple gmail,qui vous demandera vos **informations d'accès**, google va s'arranger pour enregistrer cette connexion sur votre téléphone pour que vous n'ayez plus à la refaire. Pratique mais attention. Cela signifie aussi que toutes les autres applications (même celles que vous n'utilisez pas) vont également se connecter à votre compte. Cet enregistrement de compte d'utilisateur permet à l'**ensemble des appllications** qui y sont liées de fonctionner en arrière plan sans que vous ne leur avait demandé. C'est particulièrement **intrusif** pour les applications google qui au delà de simples applications va par défaut enregistrer vos différents déplacements, vos visionnages you tube, votre navigation internet et ce même avec un VPN ! L'exemple le plus pervers est celui du playstore devenu la plateforme de téléchargement la plus populaire. Cette dernière nécessite une connexion à votre compte gmail...Vous saisissez?

- Se déconnecter d'un compte utilisateur d'arrière plan

Pour connaître et déconnecter les applications utilisant un compte de synchronisation d'arrière plan procédez comme suit :

a. Rendez vous dans les paramètres de votre téléphone
b. Accéder à la rubrique "Comptes & Synchronisation"

Vous voyez à ce moment la les différents comptes connectés.

c. Sélectionnez le compte que vous souhaitez déconnecter.
d. Appuyer sur "Plus" puis "Supprimer le compte"

Concrétement, cela ne prend que peu de temps ! Gardez ainsi la main sur les applications fonctionnant en arrière plan !

- Quoi d'autre ?

Généralement les applications qui utilisent un compte d'arrière plan sont des applications qui nécessitent une synchronisation de données par exemple une application de CLOUD comme Drive de chez Google ou facebook pour obtenir les flux de notifications. Ces applications sont souvents intrusives et à moins de pouvoir accéder au code source complet de ces applications généralement gardé au secret et ceci dans le but d'en connaitre ses activités sur votre téléphone, ne les utilisez pas.

- Synchroniser vos photos

Vos photos **personnelles** sont et doivent rester personnelles ! Toutes vos photos sont enregistrées sur votre téléphone grâce à l'application native vous permettant de réaliser des photos sur votre téléphone. Les développeurs d'applications de CLOUD ont vu dans ce stockage une opportunité absolue pour leur business car vos photos représentent beaucoup de stockage et leur argument principal s'appuie sur le sentiment de perte. C'est pourquoi il est facile d'accepter la synchronisation de vos photos sur une plateforme de CLOUD comme Google Drive. Si votre compte est piraté, la personne aura accès à vos photos et même si vous avez vidé votre téléphone de son contenu ! Pour sauvegarder vos photos, oubliez la synchronisation des plateformes de CLOUD parfois trop floues sur les **conditions de stockage**, de sécurité et de **confidentialité**. Muni d'un PC, raccordez votre téléphone avec son câble USB puis transférez vos photos sur votre disque dur personnel. C'est bien plus sécurisé !

- Les applications intrusives à éviter

Difficile de lister les applications intrusives. Partez du principe que toutes le sont. C'est pourquoi il est important de vous forcer à vous **questionner sur la réelle utilité d'une application dans votre quotidien**. Cela vous amènera, a force, à trouver des solutions alternatives aussi efficaces et moins intrusives.

D. SANS GOOGLE? C’EST POSSIBLE !

1. Introduction

Pouvoir utiliser son téléphone sans Google, c’est possible. Enfin presque. Disons qu’il faut une certaine détermination pour régler son téléphone afin d’y arriver et d’adopter son comportement vis à vis de cela. Mais pour cela, il vous faut comprendre parfaitement les mécanismes des applications google et de leur interactivités.

Voici la liste de base des applications généralement installées sur un téléphone Android :

- Google (Application de gestion de votre compte personnel google)
- Google Chrome (Naviguateur internet)
- Gmail (Messagerie email)
- Maps (GPS)
- Duo (Appel vidéo)
- PlayStore (Plateforme de téléchargement d’applications)
- You tube (Plateforme vidéo)

Ces applications sont la base des activités de Google.

Vous verrez dans les rubriques suivantes qu’il est possible de s’en passer. Tout au moins de ne pas vivre en permanence avec ces applications, réputées pour faire l’impasse sur bon nombre de principes sur la confidentialité de vos données personnelles.

2. Store d’applications alternatif

Il existe des alternatives au store d’application PlayStore.
Ces alternatives permettent de ne pas transmettre plus de données personnelles aux GAFAM, de **mieux rémunérer les développeurs** ou encore de trouver des applications introuvables sur le PlayStore.

- APK Mirror (Dépôt)
- F-Droid
- Aptoide
- Humble Bundle

F-Droid est un catalogue d’applications alternatif assez populaire, bien que peu connu du grand public. Ce projet héberge exclusivement des applications libres et *open sources*.

- Oui mais si je trouve mon application uniquement sur le PlayStore?

Hey bien, utilisez le Playstore, connectez vous, télécharger votre application puis déconnectez vous immédiatement de votre compte google d’arrière plan comme décris plus haut dans ce document. Le principal est de conserver cette habitude de toujours priviligier les alternatives de plus en plus sérieuses face au géant comme Google.

3. Navigateur internet

Le naviguateur internet est le support de référence des **GAFAM** pour connaitre vos **activités** sur le web. Si vous utlisez Google Chrome tout en étant connecté à votre compte google d’arrière plan, celui ci enregistrera tous **vos faits et gestes** permettant ainsi à Google de grossir sa base de données vous concernant pour toujours mieux vous profiler.

La recherche sur le web est généralement quotidienne. C’est pourquoi il est très important de choisir les bon outils, fiable et les plus sécurisés possible.
Il existe beaucoup d’outils. Je ne vais ici que vous présenter la configuration que j’uilise depuis plusieurs mois et qui pour moi représente la meilleure alternative. Suivez scrupuleusement ces informations. Elles sont capitales !

Cette alternative repose sur 2 éléments importants :

- Le naviguateur (Brave)
- Le moteur de recherche (DuckDuckGo)

a. Retirer le raccourci (l'icône) de google Chrome de votre première vue d'écran.

b. Télécharger l'application "Brave" sur votre plateforme d'applications et installez la sur votre smartphone.

c. Dans les paramètres de l'application Brave, rubrique "Moteur de recherche - ➔ Onglet standard", sélectionner "DuckDuckGo".

d. Dans les paramètres de l'application Brave, rubrique "Confidentialité" activez l'option "interdire le suvi"

e. Vous pouvez installer un "Widget" Brave sur votre première vue d'écran vous permettant de rechercher sur le web directement depuis cette vue.

f.Pensez à mettre brave comme naviguateur internet par défaut afin que tous les liens web que vous ouvrirez soient ouvert avec ce naviguateur. Généralement, lorsque vous cliquez sur un lien, le système demande avec quel naviguateur vous souhaitez l'ouvrir. Il vous suffit de choisir Brave et de cocher " se souvenir de mon choix".

4. Le Cloud

Le cloud s'est grandement développé depuis les 5 dernières années.
Un CLOUD est un ordinateur distant permettant de stocker vos documents, photos,contacts,messages sur un support différent de votre smartphone.
Le problème c'est qu'il impossible de déterminer avec précision comment sont utilisé vos données stockées sur ce CLOUD. A moins que vous n'ayez votre propre CLOUD auto-hébergé. J**e déconseille vivement l'utilisation d'un service CLOUD quelqu'en soit l'éditeur.**

5. Email sécurisée et chifrée

Il existe un grand nombre de service email. Le seul pour le moment qui a retenu mon attention est **protonmail** qui propose un **chiffrage** de vos emails et une politique de confidentialité accrue. Utilisez l'application Protonmail vous assure une sécurité et une confidentialité pour vos emails. Vous pouvez trouver l'application "Protonmail" sur votre plateforme d'applications favorite.

6. Conversation instantanée et sécurisée en ligne

Avec les récents scandales liée à l'application "WhatsApp" qui révèlent que bon nombre d'applications tiers détenues par Facebook sont intrusives. L'alternative gratuite du moment se nomme "**Signal**". Elle offre les mêmes fonctionnalités mais est plus sécurisée et respecte votre confidentialité, pour le moment. Cependant cette application repose sur des serveurs AWS (Amazon) et par conséquence soumise aux juridictions américaines.

L'autre alternative est **Threema**. Certe payante 1 fois 3,99€, cette application basé en Suisse propose en plus du chiffrement bout en bout constant, une réduction significative des métadonnées stockées sur leurs serveurs (votre empreinte numérique) et une conformité stricte aux réglements européenns liés à la protection des données personnelles.

L'application Messenger (Facebook) est à éviter.

E. FACEBOOK

1.Introduction

Le réseau social Facebook est devenu l'acteur majeur dans le domaine. Avec sa puissance de millions d'utilisateurs dans le monde, des gouvernements tentent maintenant d'influencer les utilisteurs. Les **puplicités**, **les censures et les influences gouvernementales y sont plus nombreuses** que jamais c'est pourquoi il faut révolutionner ce domaine et avoir le courage de ne plus l'utiliser.

Si toutefois cela vous semble très difficile, vous pouvez continuer à utiliser facebook sans vous servir de l'application et du compte d'arrière plan connecté 24h/24 sur votre téléphone.

Pour cela, connectez vous sur la version web de facebook avec votre naviguateur internet **Brave** décrit plus haut dans ce document. Vous utiliserez alors exactement les mêmes fonctionnalités avec une sécurité et confidentialité accrue sans toutefois que celles ci soient totalement préservées.

2.Les applications tiers

Facebook à agrandit sa toile en faisant l'acquisition de nombreuses applications et plateforme pour mobile. Ce phénomène lui permet d'assoire son empire pour toujours plus grossir la quantité de données vous concernant, en voici une liste non exhaustive qu'il convient d'éviter :

- Facebook
- Facebook Lite
- WhatsApp
- Hello
- Messenger
- Events
- Moments
- Mentions
- LiveStage
- MSQRD
- Instagram
- Hyperlapse
- Layout
- Bolt
- Internet.org

3.L'alternative

Pour l'avoir testé, le réseau social décentralisé "**Mastodon**" est une excellente alternative à Facebook. Bien que sa présentation et son fonctionnement soit plus proche de celui de Twitter, c'est une initiative très prometeuse car celle ci repose sur un système décentralisé. Complicant substentiellement la tâche aux organismes de censures, de publicités et d'influences. Créez un compte avec votre adresse mail sur www.mamot.fr, instance Mastodon française propulsée par la Quadrature du Net et Utilisez l'application "**Tusky**" sur votre smartphone android disponible sur votre store d'applications.

F. YOUTUBE

1.Introduction

Youtube est une plateforme vidéo archi connue. Mais la montée en puissance des publicités est un inconvénient majeur. De plus, utilisée avec un compte d'arrière plan, Google affine votre profilage pour encore mieux vous connaître. De plus, la censure y est de plus en plus présente. Les gouvernements aussi s'implique de plus en plus pour contrer les systèmes démocratiques et la réglementation électorale en vigueur en **détournant la plateforme en outil de propagande.**

La variété du contenu sur youtube est encore inégalée. C'est pourquoi, si vous souhaitez toujours utiliser la plateforme, préférez l'exellente application "**NewPipe**" vous permettant de visionner les vidéos disponibles de youtube sur une application open-source disponible par exemple sur le **store Fdroid.**

2.L'alternative

PeerTube.com est l'alternative montante et prometeuse du web. Basée comme le réseau social Mastodon sur un système décentralisée, la plateforme offre de plus en plus de contenu sans publicité. Découvrez en l'instance française propulsée par la quadrature du Net : https://video.lqdn.fr/

Vous pouvez aussi vous tourner vers la platforme **Odyssée** sur www.odysee.com enrichie régulièrement de nouvelles vidéos d'utilisateurs.