Android et ses ROM alternatives

Cet article traite des ROM android recommandées et vous propose un exemple de dé-googlisation...

➡️ Vous avez peut-être entendu dire qu'il était possible d'installer un nouveau système android sur votre téléphone ?

➡️ Vous avez peut-être entendu parler de "custom ROM" ou ROM personnalisées, ces mystérieuses distributions basées sur Android, mais ne savez pas vraiment de quoi il s'agit ?

➡️ Vous avez entendu parler d'alternatives à toutes les applications Google, etc., sans ou avec peu de traceurs, open source et parfois libres ?

Vous souhaitez libérer et dé-googliser votre smartphone (ordiphone) ?

Alors, vous êtes au bon endroit !

Si votre ordiphone le permet (nous verrons plus bas la couverture des téléphones compatibles), il vous sera possible de libérer complètement le téléphone par l'installation d'une nouvelle distribution (une nouvelle custom ROM).

Nous verrons ici les principaux avantages et inconvénients des distributions alternatives, une sélection de distributions orientées "libre", vie privée et sécurité, et enfin quelques conseils pour faciliter la libération de votre ordiphone.

Etat des lieux

Le constat

Vous pouvez donc changer votre ROM pour réduire le pistage des GAFAM et BATX, et pour autant potentiellement toujours être « espionné », potentiellement par des sociétés privées (logiciel espion Pegasus) ou des organismes étatiques, selon votre niveau d'exposition.

Il est généralement admis par la communauté d'experts en sécurité qu'un téléphone moderne est un outil d'espionnage avant tout, ayant pour « *option* » la téléphonie ! L'espionnage via la carte par exemple n'a pas de solution de contournement simple ; un des moyens les plus connus

étant de mettre le téléphone dans un emballage métallique (pochette Faraday, emballages en aluminium (par exemple de chips!), etc.) afin d'être sûr de couper toutes les communications entrantes et sortantes.

Pour davantage d'informations sur l'étendu des dangers, et les mitigations actuelles : Paf LeGeek a créé une vidéo sur ce sujet que nous recommandons pour bien comprendre.

Quant aux données personnelles, le principal risque vient aussi des actions de l'utilisateur (d'où l'importance d'une éducation au numérique et d'une amélioration de son hygiène) : le fameux facteur humain, comme par exemple ouvrir la pièce jointe d'un e-mail provenant d'une source suspecte.

Vos données personnelles aujourd'hui, les fuites...

Chapitre pour information afin de comprendre l'ampleur de la collecte et la diffusion de nos données personnelles, notamment avec l'arrivée des appareils mobiles.

La collecte des données

Le développeur hollandais Bert Hubert a conçu une application qui vous alerte quand Google collecte vos données. Sans surprise, les "bips" sont quasiment incessants, et permettent de mesurer l'ampleur du traçage.

A noter que les tests présentés dans cette publication ont été réalisés sur un navigateur web, depuis un ordinateur.

Depuis un smartphone "conventionnel" du commerce qui est "google-isé" -hors OS Android libre donc- les bips se produiraient en dehors du navigateur, à l'ouverture ou l'utilisation d'applications téléchargées depuis le Playstore, et qui incluent des pisteurs type Google Analytics. Les bips auraient lieu non-stop, étant donné qu'un Gmail est lié au système sur de tels téléphones. Il serait d'ailleurs intéressant de réaliser le test avec un smartphone dé-googlisé pour constater l'écart (on peut s'attendre à un écart d'au moins 80 à 90%, les 10 à 20% reposant sur les quelques incontournables de Big Brother, ou l'appel à une API Google via Maps ou autre).

Êtes-vous localisés par votre smartphone ?
3 milliards de smartphone localisés en temps réel

Et dans ma voiture ?
Véhicule connectés et collecte de données

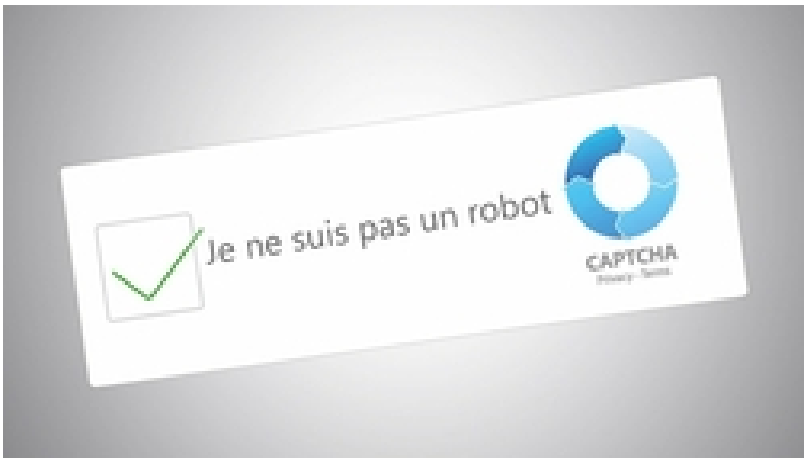
Qu'est ce qu'un site web peut collecter sur vous ?

- Pour faire le test sur votre navigateur internet

- La vidéo explicative : EFF Tools - vidéo explicative

Les captchas

- Je valide « je ne suis pas un robot » pour l'accès à certains sites



Saviez-vous que lorsque vous cochez la case "je ne suis pas un robot", ce n'est pas simplement ce fait (de cocher) qui vous authentifie à un être humain ?

En réalité, le contrôle (que vous êtes humain) consiste à vérifier dans la plupart des captchas votre historique de navigation, ainsi le site peut vérifier que vos opérations précédentes sur internet révèlent effectivement un comportement humain. Seul hic ? Une visibilité sur vos données privées sans votre consentement. En fait, c'est même vous qui en donnez l'autorisation avec cette validation ! Et évidemment, rien n'empêche alors le site de prélever ces données.

- D'où le principe de la compartimentation, par navigateur et moteur de recherche selon le type d'activités réalisés en ligne, que nous aborderons dans un article de ce wiki

Les réseaux sociaux

Nous ne mentionnons pas les réseaux sociaux comme Facebook, Instagram, Twitch et consorts, qui bien entendu collectent un maximum de données. Mais certains réseaux vont encore plus loin...

TikTok :
Vous êtes sûrement déjà au courant, mais bien entendu les utilisateurs de ce réseau sont surveillés par les instances chinoises .

Samsung :
Non moins surprenant, la collecte des données s'étend à beaucoup d'autres domaines, comme les télévisions (connectées!) : Une télévision qui vous espionne .

Un réglementation qui évolue... dans le mauvais sens ?

Décret n° 2022-1327 du 17 octobre 2022
portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion.

> Ce décret enjoint aux opérateurs de communications électroniques ainsi qu'aux personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi du 21/06/2004 de

> conserver, pour une durée d'un an, les données de trafic et de localisation respectivement énumérées au V de l'article R.10-13 du code des postes et des communications électroniques et à l'article 6 du décret du 20/10/2021.

Nous vous invitons à lire notre Manifeste pour prendre connaissance de ces aspects.

Big Brother

Le Prix Big Brother est une cérémonie de remise de prix à destination des gouvernements et des entreprises qui font le plus pour menacer la vie privée. La cérémonie est organisée par l'association Privacy International.

Son nom vient du personnage emblématique de l'État policier d'Océania dans le roman 1984 de George Orwell. Ce prix existe dans une dizaine de pays. Le 14 juillet 2021, **Doctolib** se voit décerner le Big Brother Awards.

Le retour de la censure ?

RT et Suptnik (Conflit Ukraine-Russie)

Depuis le 2 mars 2022, l'Union européenne a interdit RT France et Sputnik (sur les machines localisées en Europe). Fin août, les deux chaînes d'information diffusaient sur la plateforme Odysée. Le ministre chargé de la Transition numérique et des Télécommunications a alors demandé à Odysée de les bannir. C'est chose faite !

Rumble

Concernant Rumble, voici le tweet de Chris Pavlovski :

> *"Le gouvernement Français a exigé que Rumble bloque les sources d'information Russe. Comme @elonmusk, je ne déplacerai pas nos messages pour un gouvernement étranger. Rumble éteindra complètement la France (la France n'est pas importante pour nous) et nous contesterons la légalité de cette demande."*

Documentaires d'intérêts

Disparaître - Sous les radars des Algorithmes
ARTE (52 minutes)

Tous surveillés 7 milliards de suspects
ARTE (1h29)

Libérer son ordiphone

Avantages et inconvénients

Installer une distribution alternative ou custom ROM sur son ordiphone a bien des avantages, mais aussi des inconvénients. Passons-les en revue.

- Tout d'abord, cela permet de libérer son mobile des grandes entreprises qui pistent les utilisateurs et collectent leurs données, parfois même à leur insu, pour ensuite les exploiter en interne ou les revendre à des "Data Brokers". Pour ne citer qu'elles, les GAFAM et les BATX sont les plus connues. Certaines autres entités pourraient d'ailleurs être ajoutées : comme Huawei, Oracle, etc.
- À la place, les custom ROM privilégient le logiciel libre et open source, dont les avantages sont nombreux : pas de pistage, ni de publicité, plus de transparence sur les algorithmes et le code utilisés, le code source pouvant être audité par la communauté et les bogues de sécurité pouvant être corrigés plus rapidement. Mais les avantages des distributions alternatives pour Android ne s'arrêtent pas là. Les ROM alternatives sont développées et maintenues par des communautés qui continuent de maintenir à jour des "anciens" téléphones, qui ne sont rapidement plus maintenus par le fabricant (obsolescence programmée) ! Ils y apportent des correctifs de sécurité et de nouvelles fonctionnalités ou logiciels.
- Les distributions alternatives contiennent généralement assez peu d'applications système (celles que l'on ne peut désinstaller), afin de laisser libre choix à l'utilisateur et ne pas utiliser d'espace de stockage inutilement. Cela permet également d'améliorer la durée de vie de la batterie.

Malheureusement, l'utilisation de ROM alternatives a aussi quelques inconvénients :

- Selon les appareils et le nombre de contributeurs, des bogues peuvent apparaître, surtout lorsque la ROM que vous utilisez n'est pas supportée officiellement. Ce n'est cependant pas une généralité.
- Lors de l'installation d'une distribution alternative, il faut déverrouiller le "bootloader", ce qui implique de déverouiller le modèle de sécurité, et sur un grand nombre de téléphones, il n'est pas possible de le re-verrouiller sans la ROM d'origine ("stock ROM" en anglais).
- Enfin, certaines applications, principalement celles des banques peuvent détecter la présence d'un système alternatif, et refuser de fonctionner correctement. Il existe néanmoins des parades (microG, composant Play Services mis en "bac à sable", Magisk par exemple).

Déverouiller son Bootloader

L'article dédié à ce sujet se trouve ici : déverrouiller son bootloader.

Deux philosophies qui s'affrontent

Licence fermée ou libre ?

Les licences Propriétaires ou le Copyright

Le copyright c'est par exemple Google qui rachète tous les droits et brevets pour imposer un Android contenant ses surcouches et ajouter une identification obligatoire (le Google ID -pendant de l'Apple ID pour la marque à la pomme- via son courriel « gmail »), permettant ainsi d'en tracer les utilisateurs.

Ce sont également des développeurs qui ajoutent leur application sur le Play Store avec des traceurs pour collecter les données des utlisateurs et les monétiser.

Ce sont enfin des applications ou systèmes qui ne sont pas auditables facilement, qui n'appartiennent qu'aux entités qui les ont créés (et donc non copiables sous peine de poursuites judiciaires), et dont nous devons avoir une confiance *absolue* en ce qu'ils proposent et disent !

Libre de droits et Open-Source

Les applications ou systèmes **open source** ont leur code de développement ouvert à tous, pour utilisation libre et vérification. Le côté **Libre** (libre de droit) se réfère aux aspects éthiques. Reportez-vous au glossaire pour plus d'informations.

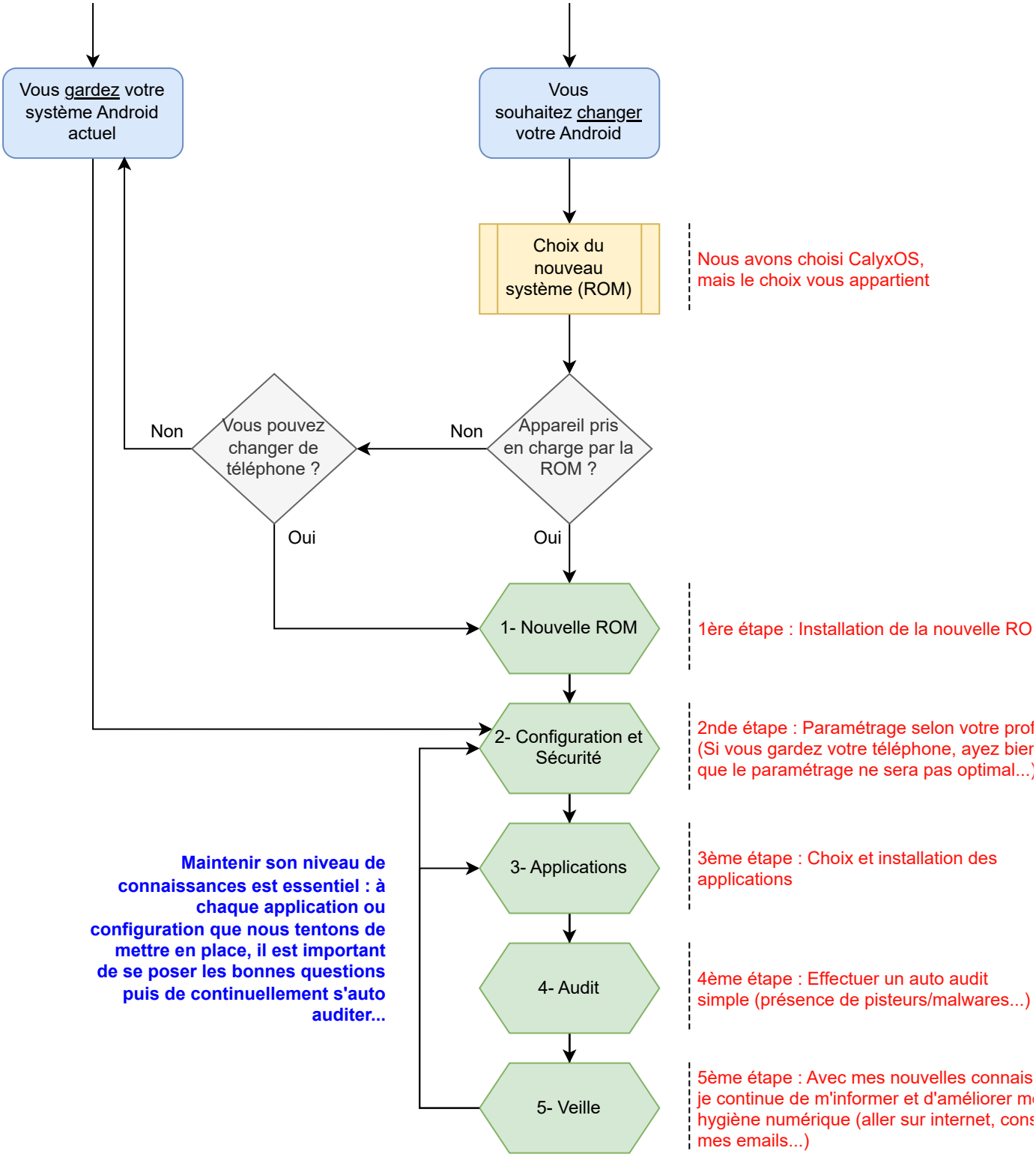
Les aspects importants de ces 2 licences sont surtout le côté « **vérifiées** » et/ou **développées** par une communauté de développeurs indépendants cherchant à faire des applications vertueuses sans tous les pisteurs et avec un modèle de licence axé sur le partage public.

A noter que le noyau même d'Android était à l'origine open source avant d'être racheté par Google (explication plus loin dans ce document).

Schéma de principe

Nous vous rappelons qu'installer une distribution alternative sur son ordiphone n'est pas sans risque ! Sauvegardez toutes données importantes avant de procéder à des modifications. Il existe un risque de "bricker" votre appareil, c'est-à-dire de le rendre inutilisable.

Lisez la page Avertissements et n'hésitez pas à vous faire conseiller auprès de la communauté.



Ci-dessous vous retrouvez nos recommandations suivant le profil.

Nous avons scindé en différents onglets :
-- L'onglet "Pour débuter" pour les débutants et nouveaux venus dans le monde Android qui ne souhaitent pas creuser le sujet.
-- L'onglet "Aller plus loin" pour ceux qui souhaitent apprendre le monde Android et une liste de ROM correspondant aux profils moins débutants.
-- L'onglet "Pour les initiés" afin d'obtenir des informations complémentaires et une

liste de ROMs correspondant aux profils initiés.

Pour débuter | Aller plus loin | Pour les initiés

ROMs conseillées

Voici les ROMs alternatives du marché que nous recommandons pour ceux qui ne souhaitent pas creuser plus avant le sujet :

Nom	Modèles supportés	Commentaire
/e/ OS	270+ Modèles supportés	Distribution qui couvre une grande partie du reste des téléphones (Offre une solution cloud eOS (1 Go) pour stocker ses courriels, not **Pour l'installation, sur le modèle de votre téléphone, cliquez sur le les indications (utilisation uniquement d'un navigateur chromium,**
Calyx OS	15 Modèles supportés	Uniquement disponible sur les Google Pixels. Privilégiez des Goog **Rendez-vous ici pour l'installation. Suivez scrupuleusement le chromium, installation des drivers, etc.)**
Graphene OS	10 Modèles supportés	Uniquement disponible sur les Google Pixels. Privilégiez des Goog **Rendez-vous ici pour l'installation. Suivez scrupuleusement le chromium, installation des drivers, etc.)**

Si vous souhaitez directement vous procurer des téléphones pré-installé, Murena (société derrière /e/OS) propose une boutique avec des téléphones clés en main. Privilégiez ces téléphones : Murena One

Dé-googliser son ordiphone

Dans un second temps, tant :

- pour ceux qui auraient pu installer une nouvelle ROM,
- que ceux qui malheureusement ne possèdent pas de téléphone pouvant accueillir une nouvelle ROM...

...vous pouvez directement passer à cette présente section qui vous donne un exemple afin de s'afranchir un maximum des services tiers des GAFAM 😃

Préambule

Cette section est un guide d'installation d'un environnement Android dégooglisé permettant de protéger du mieux possible vos données personnelles et donc d'augmenter le niveau de votre vie privée, et à certain niveau votre anonymat.

Pas à pas, vous allez configurer vous-même votre téléphone dans ce but. Ce document ne contient pas toutes les options, il y en a de toute façon trop et on s'y perdrait mais il regroupe la grande majorité des fonctionnalités utiles. Cependant nous ajoutons des liens pour ceux qui veulent approfondir.

> Ce tutoriel se scinde en 3 parties :
> ~~ Une première qui se focalise sur un système ayant pour philosophie d'utiliser MicroG (ce sera le cas pour les ROM /e/OS et CalyxOS)
> ~~ Une seconde qui s'oriente vers une implémentation modifiée des Google Play Services (Graphene OS)
> ~~ Une dernière qui propose un paramétrage en gardant sa ROM propriétaire d'origine

⚠ Notez aussi que cette branche de l'informatique est en perpétuelle évolution. Il est selon nous intéressant de toujours faire de la « veille technologique » sur ce sujet ; il existe des canaux Telegram, des sites web, des forums, etc. ; trouvez-en un et suivez l'actualité.

CalyxOS et /e/OS | GrapheneOS | ROM d'origine

Premiers paramétrages

Des paramétrages de base sont nécessaires afin de renforcer dans un premier temps la sécurité et la vie privée sur votre ordiphone :

➡ Désactiver la recherche de localisation

- *Paramètres → Localisation → Service de localisation → Désactiver pour wifi et bluetooth*

➡ Désactiver les installations du navigateur internet

- *Paramètres → Applications → Sélectionner votre navigateur web (Vanadium, Bromite, etc.) → Installation d'applis inconnues → désactiver "Autoriser cette source".*

➡ Désactiver la vérification de connectivité

- *Paramètres → Réseau & Internet → Décocher "Contrôle de connexion"*

Magasins d'applications

CalyxOS | /e/OS

CalyxOS vient avec le magasin d'application F-Droid, qui contient une grande partie des applications libres et open-sources.

➡️ Il est tout à fait possible d'ajouter un second magasin d'applications open source. Nous avons ici choisi d'utiliser *Droid-ify* pour son côté 'user-friendly' plus joli à notre goût.

➡️ Pour ceux qui ont besoin cependant d'applications propriétaires (oui il y en aura toujours un peu, des applications bancaires par exemple), vous pourrez installer un magasin qui réduira la collecte des données. Nous avons ici choisi *Aurora Store*.

Ajout du magasin « Droid-ify » :
Droid-ify est un magasin (« Store » en anglais) d'applications.
Vous pouvez installer Droid-ify depuis F-droid.

Droid-ify contient beaucoup de dépôts nativement, même si vous pouvez en rajouter bien entendu. Vous pouvez ensuite rechercher et installer les applications libres proposées dans la suite de ce document.

Ajout du magasin « Aurora Store » :
Ce magasin permet de se connecter sur le Play Store de façon anonyme ou bien avec un compte google déjà existant, même si l'on vous conseille la connexion anonyme :

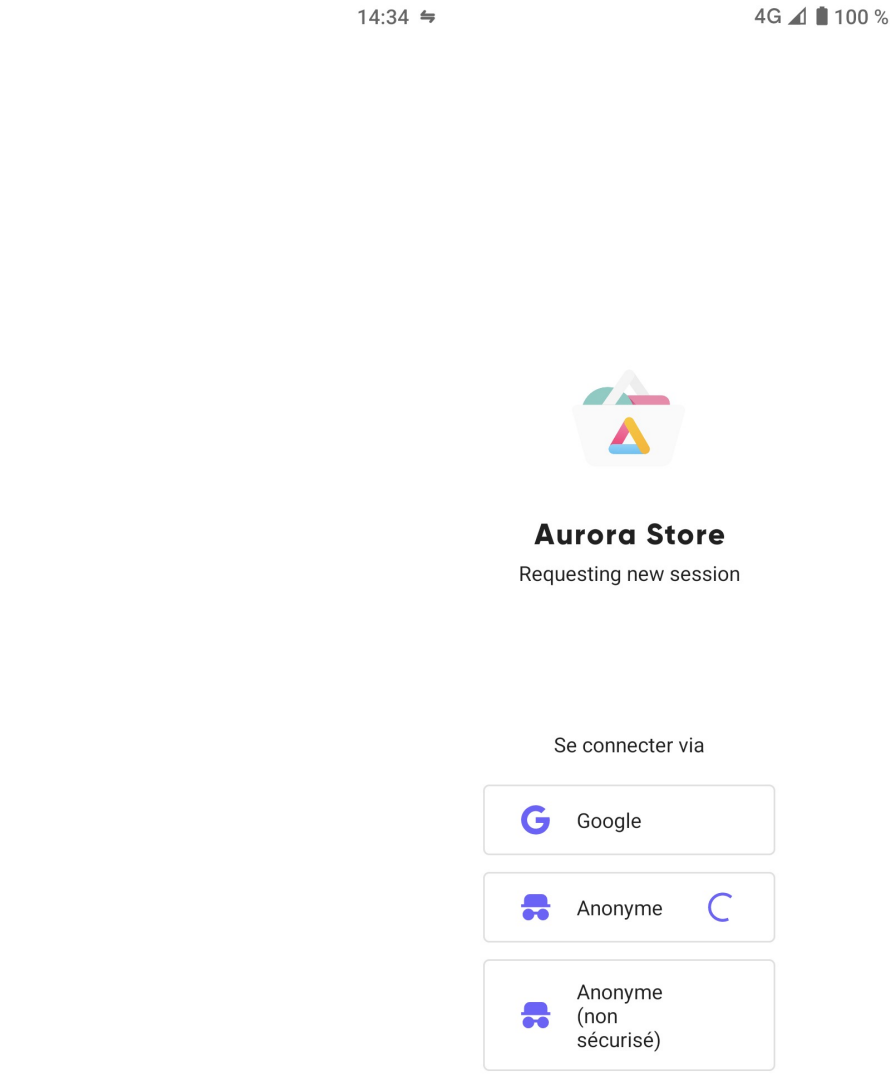
⚠ Attention : il peut arriver que la connexion anonyme ne se fasse pas, essayez dans ce cas en désactivant les VPN et/ou toutes autres fonctions utilisant la fonction VPN, comme Orbot ou DNSCrypt par exemple.

Ouvrir l'application :

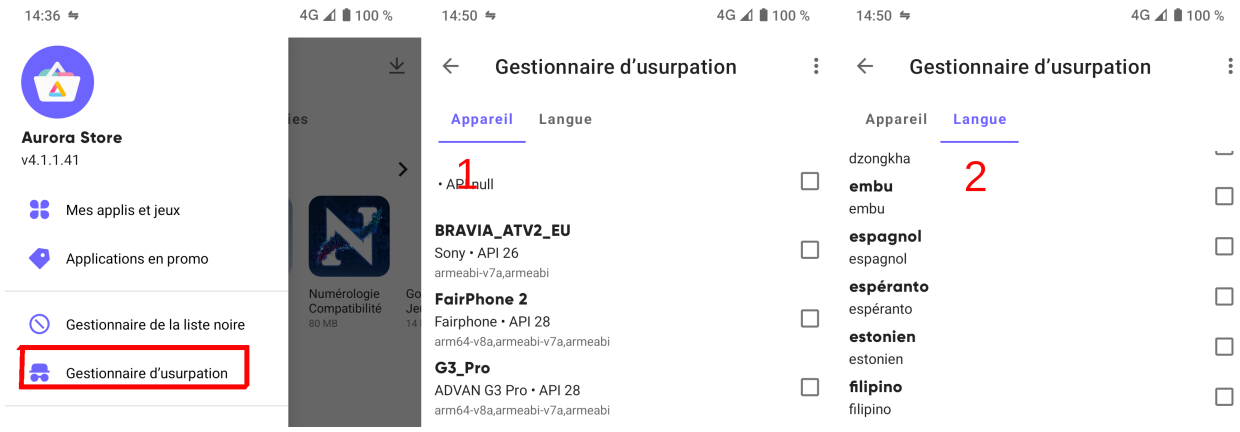
- Accepter les conditions d'utilisation (cochez la case "J'ai lu les conditions d'utilisation d'Aurora Store" puis Accepter)
- Installateur : Choisir l'option "Session installer"
- Thèmes : Choisir celui qui vous va, nous choisissons System
- Couleur : Idem
- Installateur: Accordez toutes les autorisations (les 3)

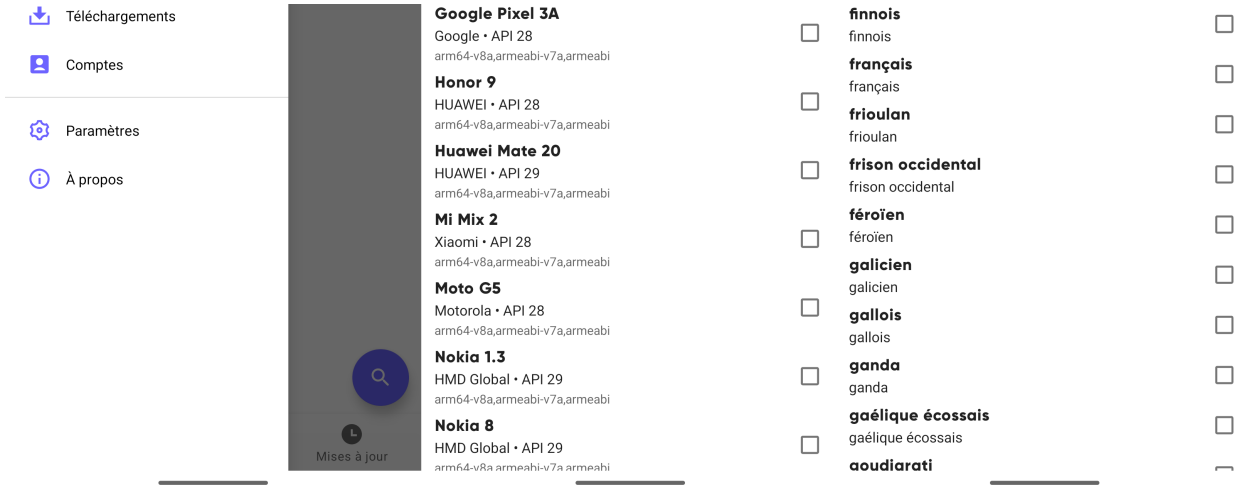
Vous arrivez ensuite à la partie authentification :

▸ Choisir compte anonyme

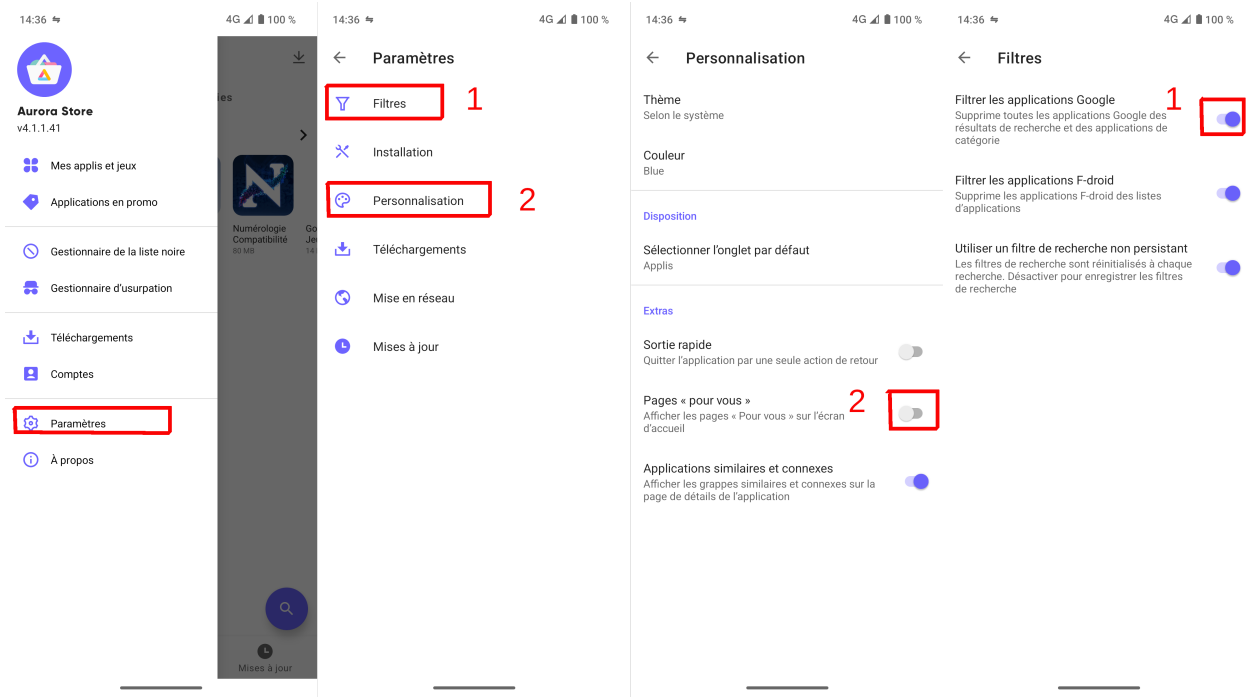


▸ Configurer le gestionnaire d'usurpation : appareil et langue





- Terminer le paramétrage :
  - Paramètres → Personnalisation → Pages "pour vous" → décocher
  - Paramètres → Filtres → Filtrer les applications Google → cocher



Applications de sécurité pré-installées

CalyxOS | /e/OS

CalyxOS étant un OS avec pour objectif de renforcer quelque peu la sécurité, il arrive avec certaines applications pré-installées.

Pare-Feu (Firewall)

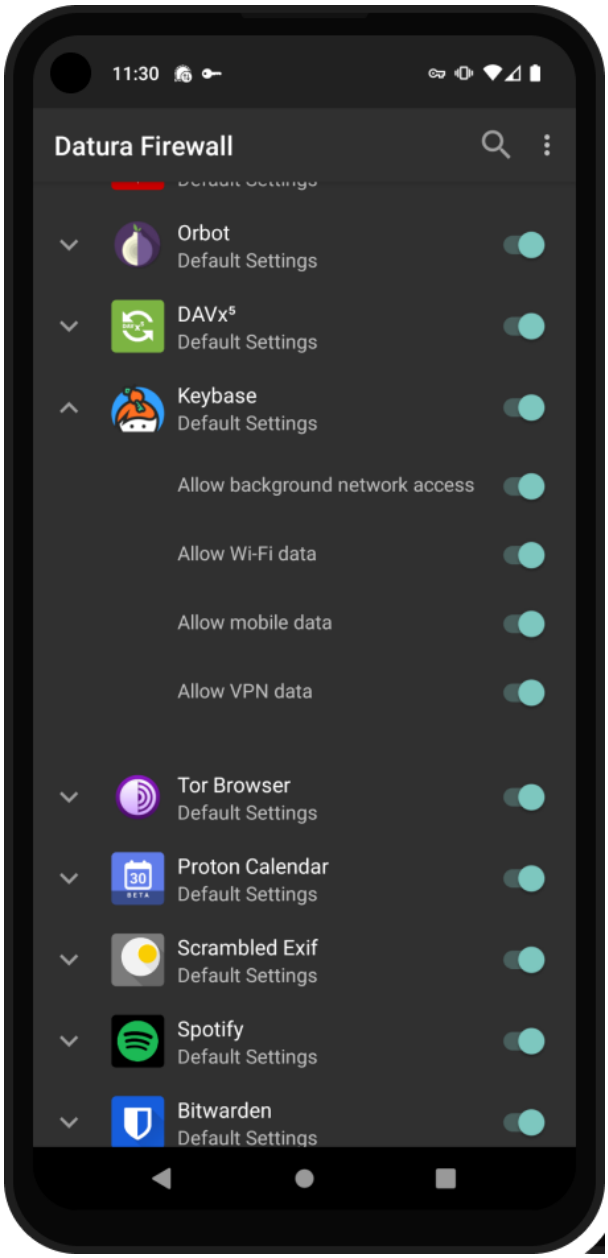
Un pare-feu (firewall) est un outil conçu pour filtrer les flux de données selon des règles que vous définissez. Autrement dit : un pare-feu permet d'autoriser (*vert*) ou d'interdire (*gris*) les accès réseaux (internet, wifi...) à une application.

Pour les applications qui n'ont pas besoin d'un accès internet : bloquez-les dans le pare-feu.

L'application native pare-feu sur CalyxOS s'appelle Datura .

Faites vos essais en lançant l'application :

- vous cochez (devient vert) : vous autorisez les accès.
- on enlève la coche (devient gris), l'application ne peut pas accéder au réseau.



👉 Avant même d'ouvrir pour la première fois une *application fraîchement installée*, prenez systématiquement pour *habitude de la bloquer dans le Pare-feu* (si l'application le permet bien sûr, c'est le cas par exemple de « Collabora Office » qui n'a pas besoin d'accéder à internet).

Il est important de faire des essais pour bien comprendre le

fonctionnement : décochez une application qui accède à internet et lancez là par exemple.

VPN

Pour le côté technique, nous vous renvoyons vers l'article dédié aux VPNs.

CalyxOS vient nativement avec deux solutions VPNs pré-installées : « Calyx VPN » qui est une application développée par les développeurs Calyx eux-mêmes et « Riseup VPN » qui est un outil créé par le collectif bien connu des activistes du même nom.

Aucun paramétrage n'est ici à entreprendre, et l'activation/désactivation se fait avec un gros bouton au centre de l'écran quand vous ouvrez l'application... plutôt simple !

Cependant attention, nous ne recommandons pas ces 2 outils (d'autant plus qu'ils souffrent de lenteurs et ne proposent que peu de serveurs), préférez ceux proposés dans l'article dédié.

Pour rappel, un VPN n'est pas un outil magique. Son rôle est orienté sécurité et vie privée et non anonymat dont c'est l'objectif de Tor.

Profil professionnel

CalyxOS | /e/OS

La configuration du profil professionnel est essentielle seulement si vous avez besoin d'isoler les applications qui viennent du « Play Store » ou d'« Aurora Store/App Lounge ».

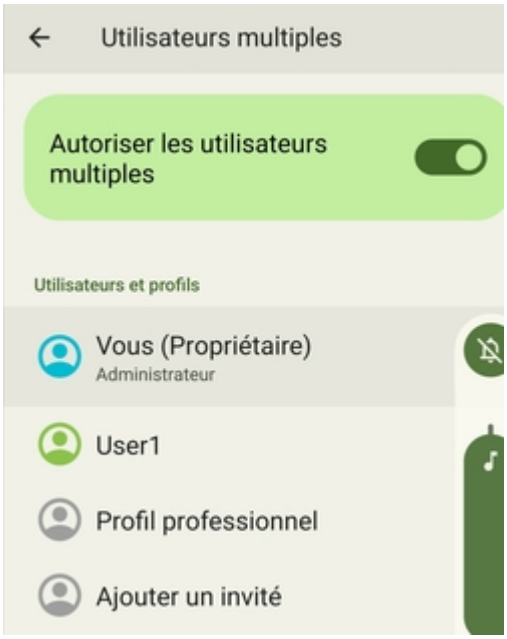
En effet ces applications contiennent pour la plupart (pour ne pas dire, toutes !) des traceurs et sont de sources propriétaires ce qui nous empêche d'avoir accès à leur code source et analyser leurs objectifs. N'installez du coup du magasin « Aurora Store/AppLounge » que le strict nécessaire et les applications non présentes sur Droid-ify (ou F-droid).

Isolées dans le profil professionnel, elles ont des droits restreints et notamment aucun accès à l'ensemble de vos fichiers et applications. Du coup, même pour lire un fichier « PDF », il faut positionner aussi le lecteur PDF dans le profil professionnel.

A noter que le profil professionnel partage le lanceur d'applications et les notifications avec l'utilisateur.

Création du profil

- *Paramètres → Système → Utilisateurs multiples → cocher : "Autoriser les utilisateurs multiples"*
- *Puis Ajoutez un profil → Profil professionnel*



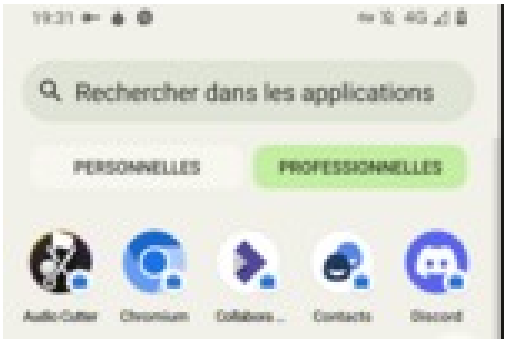
Choisir les applications pour ce profil

Une fois créé, cochez les applications qui seront installées sur ce profil.

- *Cliquez sur - Profil professionnel - et cochez chaque application qui seront disponibles dans le profil.*

Visualisation des applications

Visualiser les applications :



- Accédez au sélectionneur d'applications (sur notre téléphone : il suffit de glisser le doigt de bas en haut depuis le milieu-bas de l'écran)
- Cliquez sur « PROFESSIONNELLES » en haut à droite.

Vous avez un onglet pour les applications personnelles et un onglet pour les applications professionnelles

Vous pouvez y accéder ainsi.

> ⚠ *Potentiel problème* : si le profil professionnel n'apparaît pas dans les applications comme ci-dessus (c'est possible sur CalyxOS ou /e/OS), il faudra installer « Shelter » ou « Insular » depuis Droid-ify. Normalement ce bug a été résolu.

Désactivation des applications

Pour désactiver le profil :

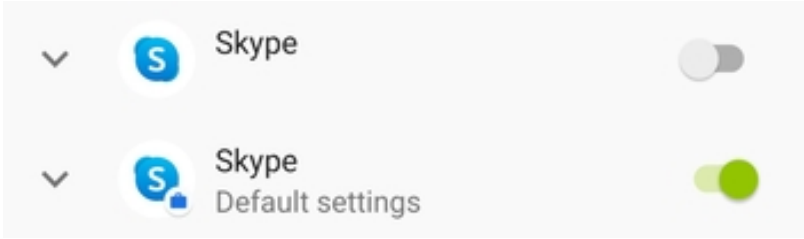
- Accédez au sélectionneur d'applications (sur notre téléphone : il suffit de glisser le doigt de bas en haut depuis le milieu-bas de l'écran)
- Cliquez sur « Désactiver les applis professionnelles » en bas à droite.

Mots de passe spécifiques

Pour éviter de se mélanger entre les différents profils, il est intéressant de choisir des mots de passe différents pour chaque profil.

- *Paramétres → Sécurité → Verrouillage du profil professionnel → puis configurer un mot de passe*

Configuration du Pare-feu



Autorisez ensuite les applications du profil propriétaire à *accéder à internet* via **l'application « Pare-feu »** (il y a un petit cadenas sur l'icône pour chaque application du profil propriétaire) et retirez les droits pour le propriétaire (il n'aura donc plus accès à internet).

Vous pouvez peaufiner ces droits (wifi, etc.) en ouvrant l'application.

Nettoyage des métadonnées

Deux applications spécifiquement développées pour les téléphones permettent de jouer sur les données EXIF : « Scrambled Exif » ou « Imagepipe » sont des applications qui peuvent supprimer les méta données (localisation, auteur, etc) des images.

La manipulation est simple : lorsque vous souhaitez partager n'importe où cette photo, partagez d"abord via l'application Scrambled Exif ou ImagePipe, puis partagez vers l'application que vous souhaitez.

Ainsi l'image passe dans une moulinette qui supprime la plupart des métadonnées avant d'être transmise ailleurs.

Navigateur internet

Les navigateurs internet pré-installés sur CalyxOS et /e/OS sont des navigateurs basés sur Bromite (forks, avec une base Chromium dégooglisée), qu'il sera nécessaire de paramétrer pour ajouter un moteur de recherche, sinon c'est Google Search qui sera votre moteur par défaut !

Ici nous avons choisi https://searx.gnous.eu/

Il y a bien entendu d'autres alternatives recommandées : que vous retrouverez ici.

Pour changer de moteur de recherche sur ces navigateurs :

- Ouvrez un onglet puis naviguez vers le moteur de recherche que vous souhaitez mettre en moteur par défaut (ici dans notre cas, nous naviguons vers https://searx.gnous.eu/
- Faites une recherche avec le moteur
- Ensuite dans les « Paramètres » du navigateur (les 3 points en haut à droite) :
  - Allez sur "Moteur de recherche"
  - Une liste vous est présentée, avec une section 'Consultations récentes' : Choisissez ici « SearX » (pour pointer sur https://searx.gnous.eu/).

> Afin de limiter au maximum le nombre d'applications installées sur Android et ainsi éviter les potentiels traceurs, il est intéressant de faire un lien (un **raccourci**) de la page web de l'application sur votre bureau plutôt que d'installer une application native. C'est moins « pratique » bien entendu, et parfois certaines applications ne seront pas utilisables (dans ce cas, vous pourrez utiliser l'application native Android), mais cela évite déjà une première phase de collecte via les applications.

Point essentiel pour le navigateur Tor :

Nous en avons déjà discuté dans l'article dédié aux outils VPN et TOR, partie Tor, pour l'utilisation sur ordinateur. Ces recommandations s'appliquent également pour les ordiphones :

- Vous pouvez utiliser le navigateur « Tor Browser » mobile pour accéder à internet via le réseau Tor, toutefois certaines fonctionnalités seront désactivées, et il ne pourra pas être utilisé dans tous les cas.
- Une autre possibilité est d'installer une application qui utilisera la fonctionnalité VPN du téléphone afin de faire passer *TOUT* le traffic réseau du téléphone via Tor. Deux

applications sont disponibles :

- Orbot qui s'utilisera comme un VPN et qui fera transiter vos requêtes sur le réseau Tor
- Invizible Pro qui propose un outil qui en plus de router votre traffic via Tor, vous permettra de choisir la protection de votre traffic DNS, ainsi que d'un accès à un autre réseau d'anonymat I2P.

> ⚠ Attention ici, vous ne pourrez plus utiliser de VPN en plus de Orbot ou Invizible, car la fonction sera déjà prise. Egalement cela reste handicapant car la vitesse s'en trouve considérablement réduite du fait des temps de latence du réseau !

Communications

SMS et Whatsapp Vs Signal / Telegram / Briar

Nous vous laissons lire l'article concernant les messageries.

Concernant les SMS, Signal a prévenu récemment que la fonctionnalité support SMS/MMS n'était plus supportée .

> " La recommandation faite par certains d'utiliser une alternative, Silence peut être envisagée... Cf. ici

Courriel

Nous savons qu'il est difficile d'abandonner une adresse courriel rapidement. C'est pourquoi dans un premier temps, vous pourrez garder vos adresses GAFAM et vous pourrez cela dit créer d'autres adresses petit à petit.

> ℹ **Pour accéder à vos comptes courriels GAFAM, n'hésitez pas à opter pour des applications tierces (K9-mail ou Fairemail) afin de limiter la collecte de vos données.**

Nous vous laissons lire l'article concernant le courriel.

Autres applications utiles

> ℹ Cette section vous propose une configuration complète pas-à-pas de certains outils que nous nommons "les essentielles" et que vous retrouvez sur les recommandations d'applications alternatives libres et open-source.

UntrackMe

Cette application permet une redirection automatique des applications telles que : YouTube, Twitter, Instagram, Reddit, Medium, Wikipedia, Google Maps, etc.

Téléchargement via F-droid

Explications : https://www.f-droid.org/en/packages/app.fedilab.nitterizeme/

Une fois installée, UntrackMe transforme les liens de ces applications afin d'être redirigé vers des alternatives **libres** telles que Nitter (pour Twitter), NewPipe (pour YouTube), Bibliogram (pour Instagram), OpenStreetMap (Google Maps), et bien d'autres.

Pour suivre des personnes sans nécessairement poster ou écrire des messages, on peut utiliser Gramhir ou Bibliogram (Instagram), Invidious (YouTube), etc.

Paramétrage de UntrackMe :
Une fois installée

- Lancez l'application
- Cliquez sur le bouton « Configurer »
- Une fenêtre Android s'ouvre. Cliquez sur « Ouvrir par défaut »
- Cliquez sur « + Ajouter un lien »
- Sélectionnez (cochez) toutes les URLs qui devront être gérées par UntrackMe
  Si vous remarquez des URLs que vous ne souhaitez faire transiter par l'application, vous pouvez très bien ne pas les cocher. Par exemple de notre côté, nous laissons décoché "t.co" car nous souhaitons que ce soit notre application Telegram qui gère ce type d'URL et non UntrackMe.
- Cliquez enfin sur « Ajouter »

Puis quittez tout.

UntrackMe gèrera maintenant toutes les URLs et vous renverra vers le bon service le cas échéant.

YouTube Vs NewPipe (ou Invidious)

Comment regarder les vidéos Youtube sans identification, c'est à dire sans connexion via un compte Gmail, sans publicité, etc... ?

NewPipe est un client qui permet de visionner ces vidéos YouTube. Via cette application vous pouvez enregistrer vos chaînes préférées, garder en favoris des vidéos, télécharger les sous-titres et des vidéos, les partager, etc.

Téléchargement depuis F-droid ou Droid-Ify.

Trois versions existent :

1. *NewPipe* (classique)
2. *NewPipe x SponsorBlock* : fork de NewPipe permettant le blocage des publicités et autres passages de vidéos promotionnels
3. *NewPipe Legacy* : pour des anciens téléphones

> Afin de ne pas diffuser des liens avec URLs Youtube, une simple manipulation est possible : nous remplaçons « https://www.youtube.com/ » par « https://yewtu.be/ » (qui est une instance Invidious). Exemple : https://www.youtube.com/watch?v=5Yqu19JOP7I devient https://yewtu.be/watch?v=5Yqu19JOP7I . Grâce à cette méthode, nous limiterons la collecte des données personnelles également de nos proches ou connaissances..

TTS (text-to-speech) eSpeak

L'installation de l'application eSpeak est possible afin d'avoir un outil TTS.

Pour configurer votre téléphone :
Paramètres → Système → Langues et saisie → Sortie de la synthèse vocale → Moteur préféré

- Choisir « espeak »

> Il existe aussi RHVoice mais pas de TTS en français, utilisation uniquement en anglais.

Audit de son téléphone

CalyxOS | /e/OS

LibreAV : Antimalware

Pour les notions techniques, référez vous à l'article sur l'hygiène numérique, partie Malware-Virus.

LibreAV est une application qui va scanner les malwares sur votre téléphone, en temps réel. Très simple d'utilisation, elle vérifiera chacune des applications que vous installerez.

> ⚠ Une fois encore nous vous avertissons, le résultat n'est pas à 100% sûr car il existe des malwares qui peuvent ne pas être détectés par des antimalwares (obfuscation des signatures, etc...).

Exodus Privacy : audit des pisteurs & autorisations

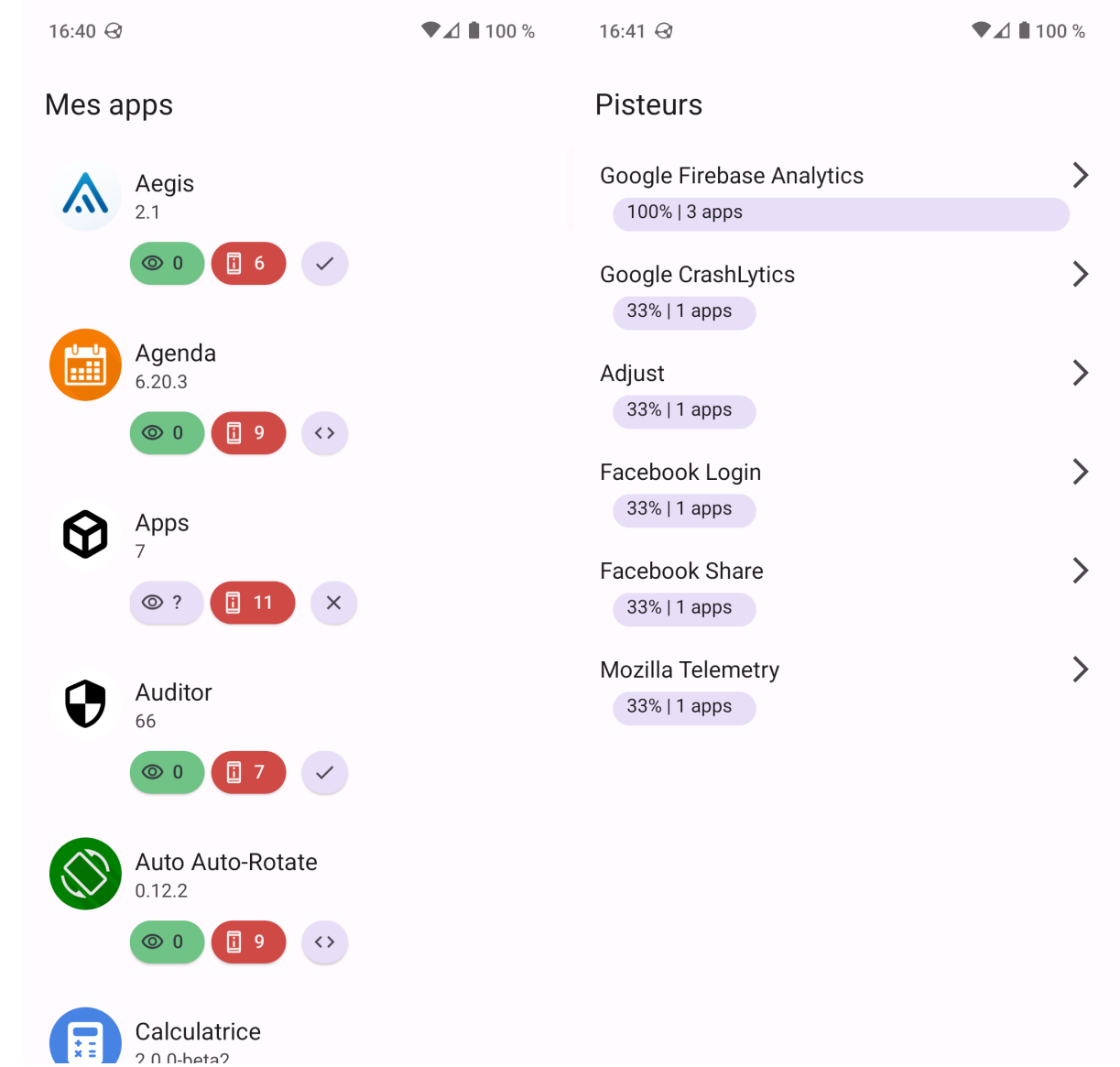
Pour faire un état des lieux des applications installées sur votre téléphone, des autorisations qui leur sont accordées, et surtout des traceurs, Exodus Privacy est un outil complet.

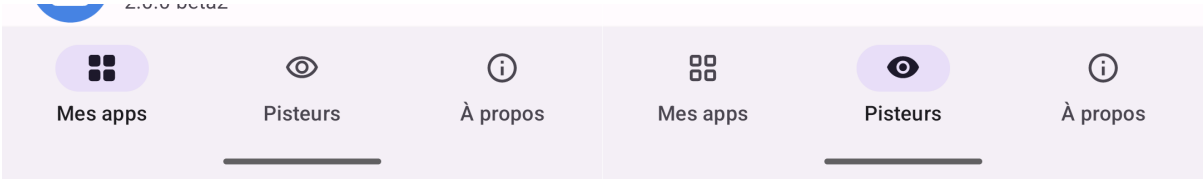
Téléchargez l'application depuis « F-droid ou Droid-ify »

- Autorisez la connexion au serveur
- Lancez l'analyse

La mise à jour des rapports Exodus se fait en glissant vers le bas (avec le doigt).

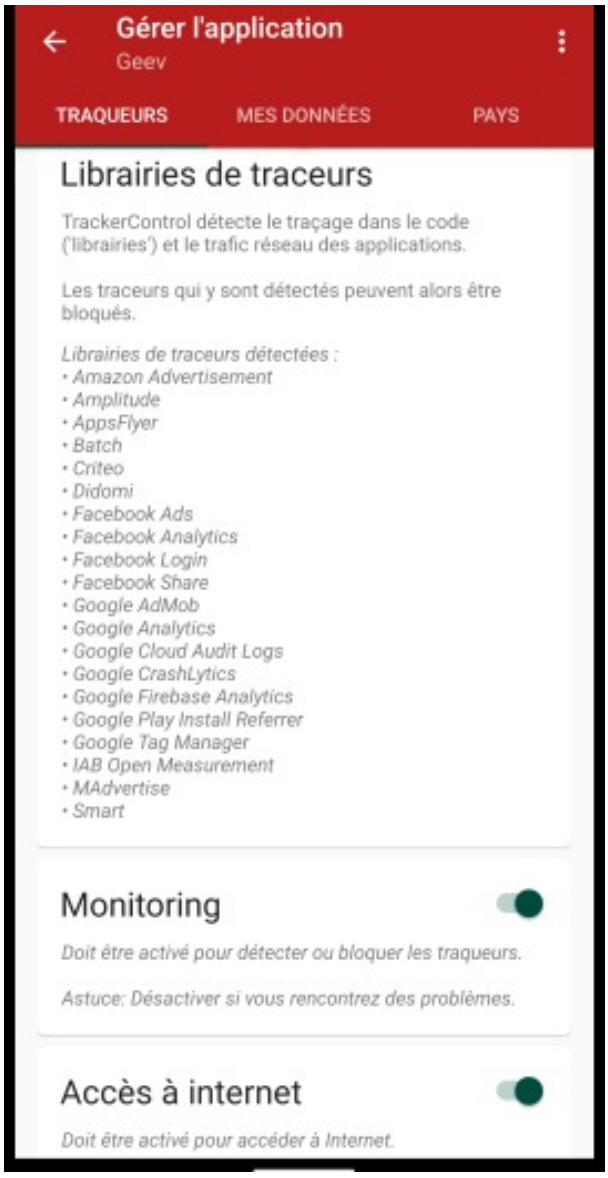
Exodus peut mettre du temps à analyser l'ensemble des applications.





> ⚠ Attention ce n'est pas parce qu'il y a 1 traceur X ou 5 permissions que l'application est de facto *mauvaise* ou *à bannir*. Il est important de prendre du recul sur les informations renvoyées et de poser vos questions à la communauté. Parfois les applications n'ont pas le choix que d'ajouter des permissions ; en revanche, il faut que cela soit justifié !

TrackerControl : contrôle la collecte cachée des données personnelles



TrackerControl est un application très puissante, parfois trop même (car bloque les connexions à certains moments !). En effet, l'application permet de détecter les traceurs, détecter les requêtes sortantes et même les bloquer (ce qui parfois bloque

complètement l'application) et de jouer finement sur la résolution des adresses.

Conclusion

Voilà, vous venez de terminer la dégooglisation de votre téléphone. Bravo !

Il reste maintenant à garder vos connaissances à jour, c'est le plus facile cela dit 😃

Pour aller plus loin

- Libérer son smartphone Android

Contributeur(s): algisowilo, Anon4952, Ayo, Nemtech, freechelmi, Yannick

Commentaires

Chargement des commentaires…