

**LIBÉREZ VOTRE ORDIPHONE
FONCTIONNANT SOUS**

ANDROID



Ce travail est sous license **Creative Commons** Attribution-ShareAlike-Non Commercial 3.0.
Il a été réalisé par teddythebest2004@europe.com

SOMMAIRE

- INTRODUCTION
- FONCTIONNEMENT ACTUEL
- MESURES DE PROTECTION
- SOLUTIONS DE CONTOURNEMENT
- CONCLUSION
- RESSOURCES DIVERSES

INTRODUCTION

INTRODUCTION

- PRÉSENTATION DU SYSTÈME ANDROID
- COMPORTEMENT DE GOOGLE

PRÉSENTATION DU SYSTÈME ANDROID



Par Définition

Android [01] est un système d'exploitation constitué d'un noyau **Linux** [02] ainsi que de quelques bibliothèques, d'une plateforme **Java** [03] et de quelques applications.

Dans la Pratique

- Il n'y a que le noyau **Linux** (sous **GNU/GPL** version 2.0 [04]) qui est totalement libre. Tout ce qui a été développé par **Google** ne l'est pas, de même que tout ce qui y est sous licence **Apache** (copyleft) [05].
- A partir de **Android** version 3, **Google** a rendu inaccessible le code qu'il y a développé (à part le noyau **Linux**). Du coup, **Android** (versions 3 et postérieures), en dehors de **Linux**, est purement et simplement constitué de logiciels privés.

(source: <https://www.gnu.org/philosophy/android-and-users-freedom.html>)

COMPORTEMENT DE GOOGLE

Les arguments de Google

- une politique de confidentialité [06] détaillée expliquant quelles données sont collectées et comment elles sont utilisées et partagées.
- des permissions d'applications [07] pour accéder à certaines données personnelles
- des contrôles de confidentialité [08] pour gérer les données personnelles comme la localisation et la navigation, les différents historiques...etc
- la transparence des données pour leur utilisation à des fins publicitaires ou d'amélioration de services
- la protection des données avec la mise en place de mesures de sécurité robustes (cryptage des données, 2FA...etc)
- un marché d'applications sécurisé [09] (certification des applications)

1/2



COMPORTEMENT DE GOOGLE

2/2

Des apparences trompeuses

Google a été impliqué dans plusieurs affaires et enquêtes liées au non-respect des données personnelles et à des violations de la vie privée.

- Des données privées ont été collectée avec les véhicules **Google Street View** [I0]
- La licence **GNU/GPL** n'a pas totalement été respectée par **Google** [I1]
- L'usage de **Safari** [I2] contourné et les données de navigation des utilisateurs collectées par **Google** [I3]
- Depuis la mise en place du **RGPD** [I4], **Google** a été plusieurs fois condamné pour non respect des données des utilisateurs en 2019 [I5], en 2020 [I6] [I7], en 2023 [I8]



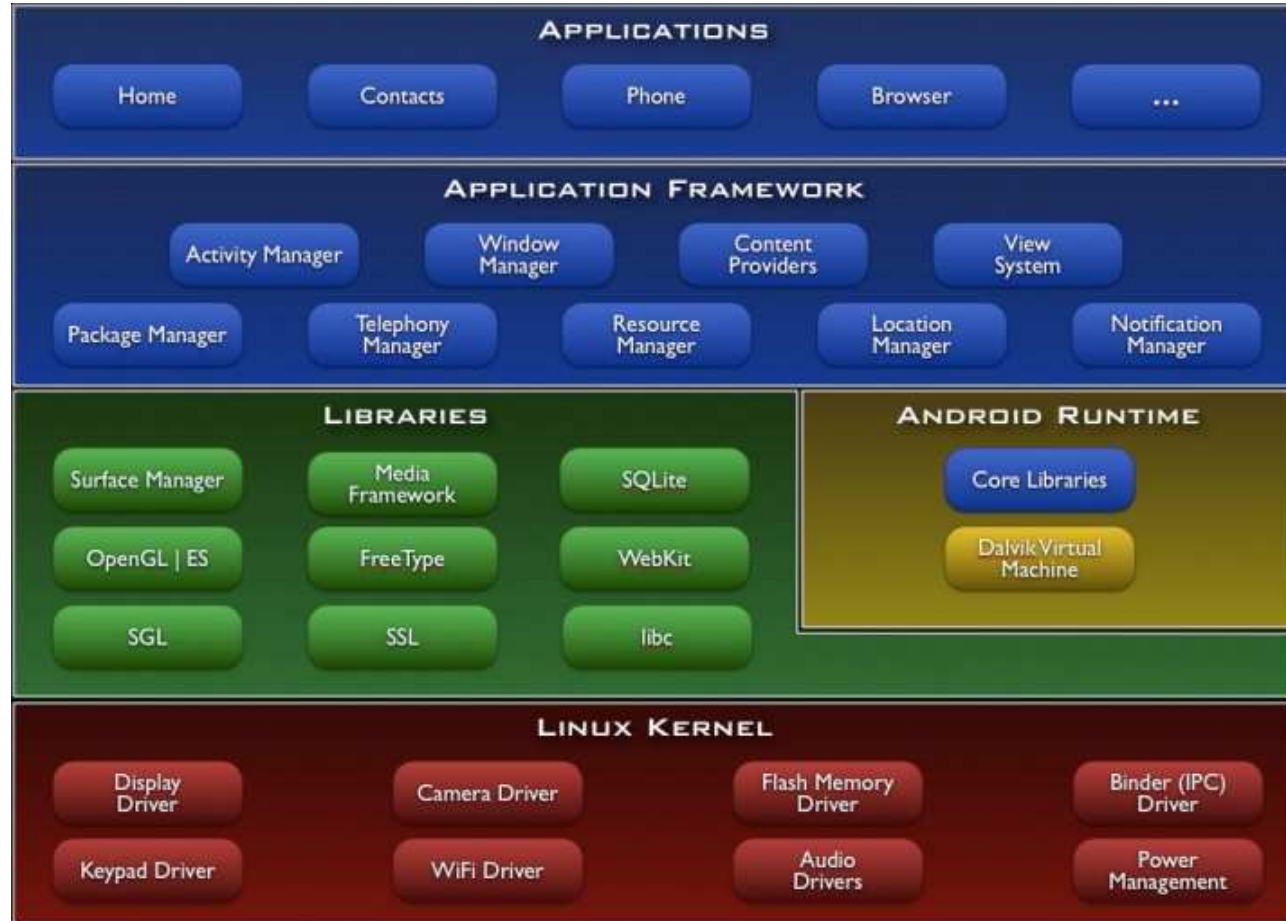
FONCTIONNEMENT ACTUEL

FONCTIONNEMENT ACTUEL

- ARCHITECTURE DU SYSTÈME ANDROID
- DONNÉES PERSONNELLES

ARCHITECTURE DU SYSTÈME ANDROID

1/3





ARCHITECTURE DU SYSTÈME ANDROID

A retenir

2/3

- *Couche Applications* : applications fournies par le fabricant, celles fournies par l'opérateur, celles installées par l'utilisateur
- *Couche Gestionnaire d'Applications* : programmes de gestion des applications tels les notifications, la téléphonie, la gestion des fenêtres et interfaces, les paquets...etc
- *Couche Bibliothèques* : gestionnaires liés au fonctionnement de l'affichage, les comportements tactiles, les codecs des médias, les polices, les bases de données des applications...etc
- *Couche Système* : noyau Linux avec les différents pilotes (USB, Wifi, Bluetooth...etc)

Des informations sont disponibles à propos de cette architecture sous plusieurs formes (documents [19], vidéos [20]...etc)



ARCHITECTURE DU SYSTÈME ANDROID

Menace pour les utilisateurs 3/3

Google, fabricants et opérateurs vont pouvoir intervenir, à chacun de ces niveaux, en modifiant certaines bibliothèques, applications...etc ou en ajoutant les leurs.

Évidemment, sous prétexte de protéger leurs utilisateurs, ceux-ci n'ont qu'un accès limité à ces fonctionnalités et n'ont, surtout pas, leurs mots à dire dans le meilleur des cas ; ou sont espionnés dans le pire. Quelques fois, ce sont l'état, le gouvernement ou la Police qui interviennent et effectuent ces modifications.

Dans tous les cas, les utilisateurs n'ont qu'en partie accès et il reste, pour eux, indispensable de protéger leurs données personnelles.

LES DONNÉES PERSONNELLES

1/4

C'est quoi ? ^[21]

Elles ont plusieurs origines :

- Origine individuelle (Nom, Prénom, Adresse, Ville, N° de téléphone...etc)
- Origine technique (IMEI, N° de série, GPS...etc)
- Origine applicative (paramètres des applications: Contacts, Calendrier...etc)

Où sont-elles ?

Elles sont localisées en plusieurs endroits :

- Chez l'opérateur (Nom, Prénom, Adresse, Ville, N° de téléphone...etc)
- Sur les composants matériels (IMEI, N° de série, Adresse MAC...etc)
- Sur la carte SIM (contacts, calendrier, SMS...etc)
- Sur des serveurs distants (Google, fabricants, distributeurs...etc)



LES DONNÉES PERSONNELLES

Qui et comment y accéder ?

- ***Vous*** : par vos paramètres, journaux, applications...etc
- ***Opérateurs*** (Bouygues, Orange, SFR...etc) : par les applications installées, par les appels sur les bornes d'accès...etc
- ***Google*** : par les applications installées, le PlayStore...etc
- ***Fabricants*** (Samsung, Xiaomi, Google..etc) : par les applications et les packages installés
- ***Tiers*** (Facebook, Twitter, Instagram...etc) : par les applications installées
- ***Etat*** (Police, Gouvernement..etc) : via les serveurs des opérateurs
- ***Pirates*** : par des applications malveillantes, des failles de sécurité...etc



LES DONNÉES PERSONNELLES

Transmissions de données

- **Légalement**, tout se base, principalement, sur le consentement de l'utilisateur et est directement lié à des règles européennes (RGPD [22]) ou des pactes internationaux (Privacy Shield [23], TAFTA/TTIP [24]...etc)
- **Discrètement**, Google, distributeurs, fabricants et opérateurs vont pouvoir surveiller les différents agissements de l'utilisateur ainsi que ses données personnelles en intégrant dans leur code des pisteurs, traqueurs et profileurs [25]
- **Illégalement**, par des individus malintentionnés à travers l'exploitation de failles logicielles, de programmes malveillants ou de la crédulité de l'utilisateur



LES DONNÉES PERSONNELLES

4/4

Surveillance de masse ^[26]

Depuis la loi renseignement ^[27] de Juillet 2015, l'état, le gouvernement, la Police, sous prétexte de la sécurité intérieure et de la lutte contre le terrorisme, ont mis en place des systèmes d'écoute (officiels ou non): black-box chez les opérateurs, IMSI Catchers ^[28]...etc

L'utilisateur est contraint d'utiliser des techniques de contournement lui permettant de protéger ses données personnelles:

- Techniques de détection
- Techniques de dissimulation
- Techniques de chiffrement des communications



MESURES DE PROTECTION

MESURES DE PROTECTION

- PARAMÉTRAGES DU SYSTÈME ANDROID
- PARAMÉTRAGES DES APPLICATIONS

Android system recovery (3e)

Volume up/down to move highlight:
power button to select.

reboot system now

apply update from external storage

wipe data/factory reset

wipe cache partition

apply update from cache



PARAMÉTRAGES DU SYSTÈME ANDROID

Les smartphones **Android** disposent tous de réglages paramétrables à différents niveaux. Ces réglages sont directement liés aux valeurs des informations issues de leurs composants (localisation 2D avec la puce GPS, localisation 3D avec la puce gyroscopique, aperçus des caméras, localisation GPRS...etc)

- **Données biométriques** : La reconnaissance faciale et les empreintes digitales sont à éviter. Ces données étant enregistrées sur le smartphone, elles pourraient être utilisées à des fins malveillantes.
- **Données de sécurité** : Effectuez vos mises à jour de sécurité (sauf cas exceptionnel) Interdisez le traçage du mobile (il y a des solutions de contournement) Si une carte SD est présente, veillez à ce qu'elle soit chiffrée.
- **Mode de déverrouillage** : Optez pour un verrouillage du smartphone par code ou par schéma de déverrouillage
- **Gestionnaire d'autorisations** : Autorisez ou non les accès des applications à certaines données comme le stockage, les photos...etc ; ou encore à émettre des notifications

Plusieurs articles ont été écrits sur les paramétrages des smartphones **Android** dont celui de **Clubic** [29] ou ceux de **Google** [30].

DÉMONSTRATION



Entrer le code PIN

Votre code PIN contient au moins 4 chiffres.

1

2

ABC

3

DEF

4

GHI

5

JKL

6

MNO

7

PQRS

8

TUV

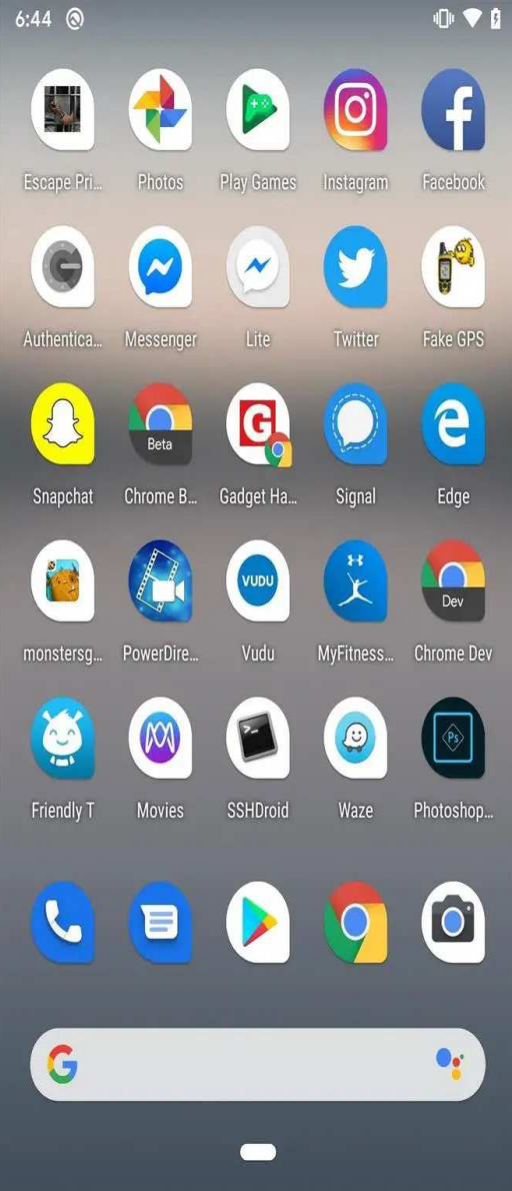
9

WXYZ



0

OK



PARAMÉTRAGES DES APPLICATIONS

Dès l'instant où une application communique avec des serveurs distants, elle transmet des données; elle nécessite donc d'être paramétrée.

- *Paramétrages Généraux* : **Google** [31], tout comme **Samsung** [32], donne quelques explications sur ces paramétrages généraux.
- *Paramétrages Individuels* : Pour chaque application, il peut y avoir des paramétrages individuels spécifiques.
- *Paramétrages Google* : Plusieurs paramètres du compte de l'utilisateur vont permettre à **Google** d'établir un profil comportemental précis (historique des positions [33], localisation du smartphone [34], traçage [35]....etc)

Ce qui est préférable, pour un utilisateur, c'est de préférer des applications indépendantes à celles des principaux acteurs corrompus (**Google** ou consorts).

Voici quelques exemples de paramétrages d'applications.

DÉMONSTRATION



SOLUTIONS DE CONTOURNEMENT

SOLUTIONS DE CONTOURNEMENT

- MARCHÉ D'APPLICATIONS LIBRES
- HÉBERGEURS DE CONFIANCE
- SYSTÈME D'EXPLOITATION

MARCHÉ D'APPLICATIONS LIBRES 1/4

Le marché d'applications

- **F-Droid** ^[36] est un magasin d'applications (communément appelé Store) libres ou Open Source ^[37] pour les systèmes d'exploitation **Android** et dérivés. Il est recommandé par la **Free Software Foundation** ^[38] ^[39]
- Il ne nécessite pas de compte, contrairement au **Play Store** et n'envoie aucune donnée permettant d'identifier l'utilisateur
- Il propose diverses applications dont certaines sont des alternatives libres de leurs équivalents privés, la plupart d'entre elles gratuites
- Les applications permettent également d'accéder à leur code source ; ce qui permet ainsi de vérifier qu'elles ne contiennent pas de traqueurs, de pisteurs ou de profileurs

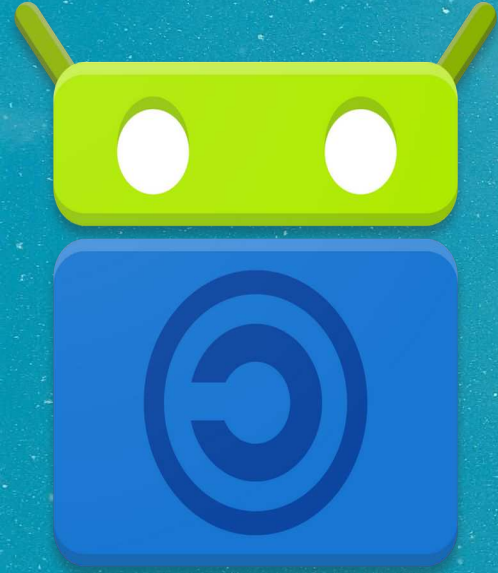


Installation de F-Droid

- Comme indiqué dans le précédent chapitre, vous devrez permettre à votre smartphone d'installer des sources inconnues [40] pour pouvoir installer **F-Droid**
- Ensuite, il faut aller sur le site de **F-Droid** afin d'y trouver l'apk et la télécharger [41]
- Enfin, il faut installer cette apk

Quelles applications Installer en 1^{er} ?

- Sans hésiter, **Exodus Privacy** [42] Grâce à elle, vous allez pouvoir vérifier si il y a des applications qui vous pistent et vous profilent et ensuite procéder à un ménage dans celles que vous conserverez et celles que vous supprimerez.
- Ensuite, **Blokada** [43] Grâce à elle, vous allez pouvoir bloquer divers publicités qui rendent pénible votre navigation sur internet



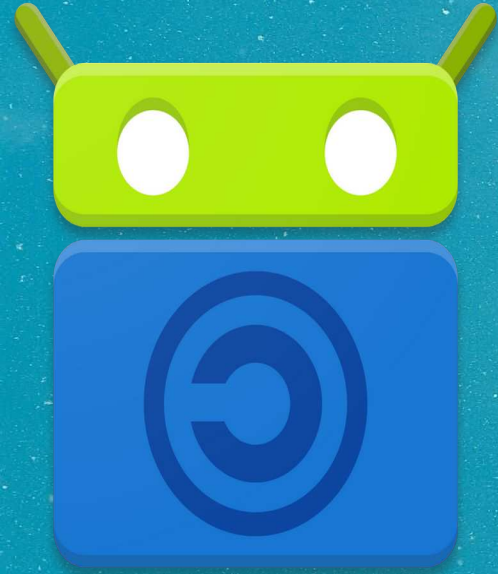
Trouver des alternatives Libres

Il faut bien faire la différence entre les applications dépendant de services non libres ou liées plus ou moins directement aux **GAFAM** [44]

Services Privateurs

Voici quelques exemples d'applications, elles sont nombreuses sur **F-Droid** :

- Acrobat Reader Cool Reader, MuPDF Mini
- Facebook MaterialFBook, Face Slim
- Gmail K-9 Mail
- Google Chrome DuckDuckGo Privacy Browser, Firefox
- Google Maps OsmAnd, Gmaps VW
- Google PlayStore Aurora Store
- MS-Office OpenDocument Reader, LibreOffice Reader
- Spotify Spotube, Spotifyer
- Telegram Nekogram X, Telegram FOSS
- Twitter X Squawker, Quawker
- YouTube NewPipe, LibreTube

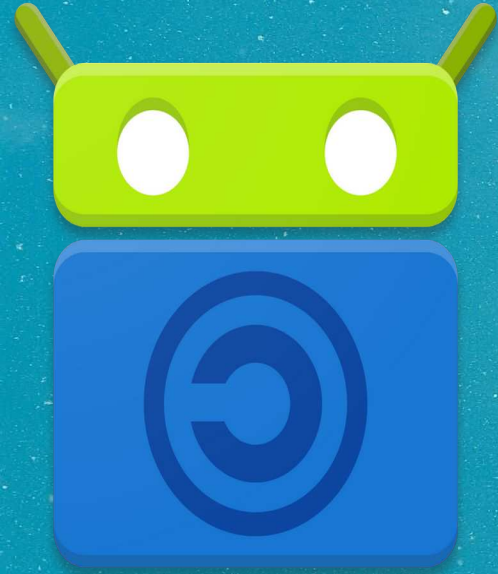


MARCHÉ D'APPLICATIONS LIBRES 4/4

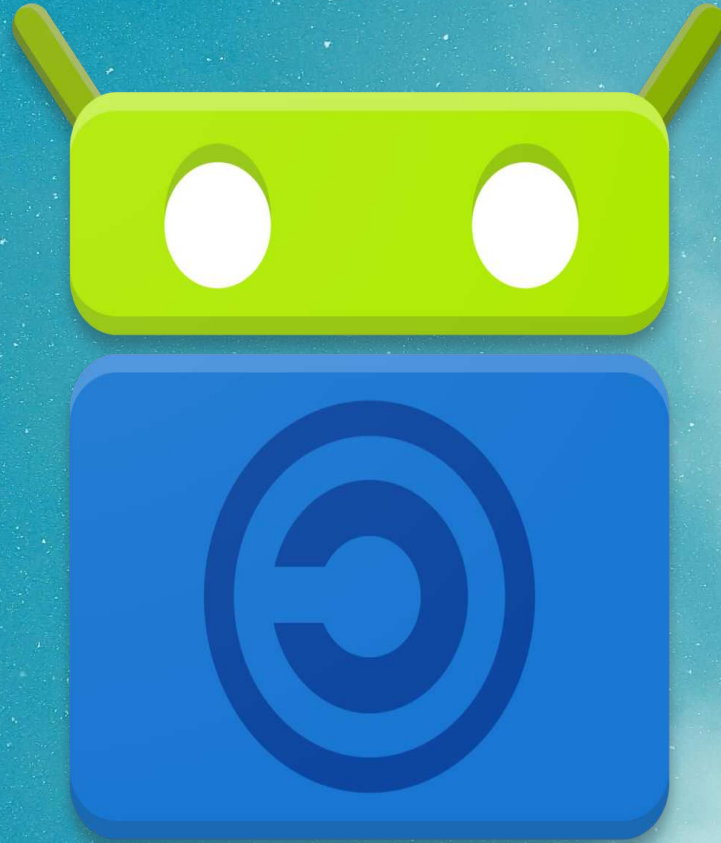
Services Libres ou Open Source

Voici quelques exemples d'applications, elles sont nombreuses sur F-Droid :

- Analyse de traçage TrackerControl, ClassyShark3xodus
- Anonymat Orbot, Tor Browser
- Calendrier Simple Calendar Pro
- Chiffrement OpenKey-chain
- Contacts Simple Contacts Pro, Simple Contacts Pro SE
- Flux RSS News Reader, spaRSS
- Lecteur Multimédia VLC, Vanilla Music
- Messagerie Jitsi Meet, Conversations
- Navigateur Free Browser, Simple Contacts Pro SE
- Réseaux Sociaux Tusky, Fedilab
- Synchronisateur DavX 5, IcsX 5
- Terminal Terminal Emulator, Termux
- Transports pMetro, Transportr



DÉMONSTRATION



HÉBERGEURS DE CONFIANCE

La solution d'hébergement de vos données personnelles passe par des serveurs **NextCloud** [45], une véritable alternative à **GoogleDrive** [46]. Elle vous permettra d'héberger vos contacts, votre calendrier...etc Toutes vos données y seront chiffrées [47].

Framasoft [48] propose une solution appelée **Framagenda** [49] ; mais, il n'est pas le seul : **Clawd** [50] propose la même chose et il est membre des **Chatons** [51] et il en existe d'autres !

Attention ! Cet hébergement nécessite l'installation, sur le smartphone, de l'application **Davx** [52] pour le calendrier et les contacts, **LePas** [53] pour vos photos



Framasoft



Une fausse idée...

Les principaux fabricants de smartphones proposent des matériels à base de systèmes privés et non respectueux des utilisateurs (système **Android**) et y rajoutent également leurs propres applications, elles-aussi non respectueuses. Et comme ces fabricants dominent le marché, l'utilisateur n'a que peu de choix.

En réalité, c'est faux !

Il existe des fabricants ou des fournisseurs de smartphones qui ont des principes éthiques. Les principales sociétés et distributeurs qui suivent ces principes sont **Technoethical** ^[54] (il ne vend pas que des smartphones) et **Fairphone** ^[55]

Mais, il en existe bien d'autres :

- **Murena** ^[56],
- **Pine64** ^[57],
- **Purism** ^[58]

Fais le toi-même !

Cette traduction de « Do it yourself ! » correspond au fait qu'il est possible de disposer d'un smartphone éthique à partir d'un modèle privateur existant. Pour cela, il faut installer un système d'exploitation éthique.

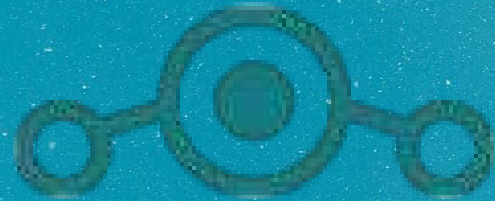
Plusieurs articles ont été écrit à propos de migration vers d'autres systèmes d'exploitation dont celui de la **Free Software Foundation** [59] ou encore celui de **Nextpit** [60] qui sont très intéressants.

Les 2 principaux systèmes d'exploitation alternatifs et qui sont recommandés par **Free Software Foundation** sont **Replicant** [61] (totalement libre) et **Lineage OS** [62] (contenant des pilotes privateurs).

Mais, il en existe d'autres :

- **/e / OS** [63],
- **Graphene OS** [64]

Vous avez le choix [65] [66]



Un peu de technique

Il y a quelques contraintes qu'il sera probablement nécessaire de contourner :

- Beaucoup de smartphones disposent d'un boot loader [67] [68] qui s'active lors de leur démarrage. Il sera peut-être nécessaire de le configurer pour qu'il puisse utiliser le système d'exploitation alternatif
- Certains smartphone nécessitent d'être rootés [69] pour pouvoir utiliser toutes les fonctionnalités proposées par le système d'exploitation alternatif

Changer de système d'exploitation demande des manipulations techniques mais de nombreuses aides existent ; comme celles pour **Lineage OS** [70] [71] [72] ou encore **Replicant** [73]. Mais, il doit en exister aussi pour d'autres systèmes...

Android system recovery <3e>

Volume up/down to move highlight;
enter button to select.

reboot system now

apply update from ADB
apply update from sdcard
apply update from cache
wipe data/factory reset
wipe cache partition
backup user data
restore user data

No command.

CONCLUSION

N'OUBLIEZ PAS QUE :

**VOS DONNÉES SONT PRÉCIEUSES ; C'EST UN VÉRITABLE
TRÉSOR POUR CEUX QUI VOUS SURVEILLENT :
PROTÉGEZ-LES !**



**VOS DONNÉES VOUS
APPARTIENNENT ET VOUS EN ÊTES
LES SEUL-E-S PROPRIÉTAIRES !**

**ET NE SACRIFIEZ JAMAIS VOS DROITS
AU DÉTRIMENT DE VOTRE LIBERTÉ !**

RESSOURCES DIVERSES

OUVRAGES PAPIER

Smartphones Android pour les nuls

Édition du 29/09/2022

Auteur : Dan Gookin

Éditeur : First Interactive

EAN: 9782412082164



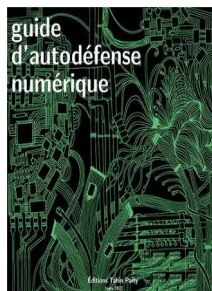
Guide d'autodéfense numérique

Édition du 24/02/2023

Auteur : Collectif

Éditeur : Tahin Party

EAN: 9782912631053



FILMS

Citizen Four

Réalisé le 10/10/2014

Réalisateur : Laura Poitras

Type : Documentaire

Résumé : Documentaire américain sur Edward Snowden et ses révélations sur l'espionnage de la NSA.



Nothing to hide

Réalisé le 08/02/2017

Réalisateur : Marc Meillassoux et Mihaela Gladovic

Type : Documentaire

Résumé : Documentaire franco-germanique sur la surveillance de masse sur les individus et la société.



RÉFÉRENCES EXTERNES

1/5

[01] <https://fr.wikipedia.org/wiki/Android>

[02] <https://fr.wikipedia.org/wiki/Linux>

[03] [https://fr.wikipedia.org/wiki/Java_\(langage\)](https://fr.wikipedia.org/wiki/Java_(langage))

[04] <https://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

[05] <https://www.apache.org/licenses/LICENSE-2.0.html>

[06] <https://policies.google.com/privacy?hl=fr>

[07] <https://support.google.com/googleplay/answer/9431959?hl=fr>

[08] <https://support.google.com/android/answer/13985942?hl=fr>

[09] <https://support.google.com/googleplay/answer/2812853?hl=fr>

[10]

<https://www.zdnet.fr/actualites/google-street-view-la-collecte-de-donnees-personnelles-pas-une-erreur-selon-une-enquete-39771322.htm>

[11] <https://www.numerama.com/politique/18353-google-accuse-d-avoir-enfreint-la-licence-gpl-avec-android.html>

[12] <https://www.apple.com/fr/safari/>

[13] <https://www.zdnet.fr/actualites/google-soupconne-d-indiscretion-a-l-egard-des-utilisateurs-de-safari-39768702.htm>

RÉFÉRENCES EXTERNES

2/5

- [14] <https://afcdp.net/reglement-europeen-rgpd-indexe-commenter/>
- [15] <https://www.quechoisir.org/actualite-donnees-personnelles-pourquoi-la-cnil-a-sanctionne-google-si-lourdement-n63167/>
- [16] https://www.lemonde.fr/pixels/article/2020/12/10/la-cnil-inflige-des-amendes-a-google-et-amazon-pour-non-respect-de-la-legislation-sur-les-cookies_6062860_4408996.html
- [17] <https://www.conseil-etat.fr/actualites/cookies-publicitaires-google-definitivement-condamne-a-payer-100-millions-d-euros>
- [18] <https://www.cnil.fr/fr/cloture-de-linjonction-prononcee-lencontre-de-google-o>
- [19] https://www-igm.univ-mlv.fr/~dr/XPOSE2008/android/archi_comp.html
- [20] <https://invidious.fdn.fr/watch?v=BW8U7wJCibo>
- [21] https://fr.wikipedia.org/wiki/Donn%C3%A9es_personnelles
- [22] <https://www.cnil.fr/fr/les-bases-legales/consentement>
- [23] https://fr.wikipedia.org/wiki/Bouclier_de_protection_des_donn%C3%A9es_UE-%C3%89tats-Unis
- [24] https://fr.wikipedia.org/wiki/Partenariat_transatlantique_de_commerce_et_d%27investissement
- [25] https://fr.wikipedia.org/wiki/Pistage_web
- [26] <https://fr.wikipedia.org/wiki/Surveillance>
- [27] <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000030931899>
- [28] <https://fr.wikipedia.org/wiki/IMSI-catcher>
- [29] <https://www.clubic.com/tutoriels/article-890091-1-comment-configurer-maintenir-smartphone-android.html> [27]
- [30] <https://support.google.com/android/answer/9083864?hl=fr>

RÉFÉRENCES EXTERNES

3/5

- [31] <https://support.google.com/android/answer/9431959?hl=fr>
- [32] <https://www.samsung.com/fr/support/mobile-devices/comment-gerer-les-parametres-des-applications/>
- [33] <https://support.google.com/accounts/answer/3118687?hl=fr>
- [34] <https://support.google.com/accounts/answer/3467281?hl=fr>
- [35] <https://support.google.com/accounts/answer/3467281?hl=fr>
- [36] <https://fr.wikipedia.org/wiki/F-Droid>
- [37] https://fr.wikipedia.org/wiki/Open_source
- [38] https://fr.wikipedia.org/wiki/Free_Software_Foundation
- [39] <https://www.fsf.org/>
- [40] <https://www.tutoriels-android.net/2012/04/comment-autoriser-les-sources-inconnues.html>
- [41] <https://f-droid.org/F-Droid.apk>
- [42] https://f-droid.org/fr/packages/org.eu.exodus_privacy.exodusprivacy
- [43] <https://blokada.org/>
- [44] <https://fr.wikipedia.org/wiki/GAFAM>
- [45] <https://fr.wikipedia.org/wiki/Nextcloud>
- [46] <https://drive.google.com/?hl=fr>
- [47] https://docs.nextcloud.com/server/latest/user_manual/fr/files/encrypting_files.html

RÉFÉRENCES EXTERNES

4/5

- [48] <https://framasoftware.org/fr/>
- [49] <https://framagenda.org/>
- [50] <https://clawd.fr/>
- [51] <https://www.chatons.org/>
- [52] <https://www.davxs.com/>
- [53] <https://f-droid.org/packages/site.leos.apps.lespas/>
- [54] <https://tehnnoetic.com/index.php?route=product/category&path=59>
- [55] <https://www.fairphone.com/fr>
- [56] <https://murena.com/smartphones/>
- [57] https://pine64.org/devices/#phones_and_tablets
- [58] <https://puri.sm/products/liberty-phone/>
- [59] <https://fsfe.org/activities/android/liberate.fr.html>
- [60] <https://www.nextpit.fr/meilleures-rom-customs-android>
- [61] <https://replicant.us/>
- [62] <https://lineageos.org/>
- [63] <https://e.foundation/e-os/>
- [64] <https://grapheneos.org/>
- [65] <https://infoidevice.fr/les-5-meilleures-alternatives-android-pour-liberer-votre-smartphone-de-google>

RÉFÉRENCES EXTERNES

s/s

- [66] <https://itsfoss.com/open-source-alternatives-android/>
- [67] https://fr.wikipedia.org/wiki/Chargeur_d%27amor%C3%A7age
- [68] https://en.wikipedia.org/wiki/Booting_process_of_Android_devices
- [69] https://fr.wikipedia.org/wiki/Root_d%27Android
- [70] <https://www.phonandroid.com/comment-installer-lineage-os-smartphone-android.html>
- [71] <https://www.androidauthority.com/lineageos-install-guide-893303/>
- [72] <https://wiki.lineageos.org/>
- [73] <https://redmine.replicant.us/projects/replicant/wiki/>
- [74] <https://fr.wikipedia.org/wiki/Hacktivisme>
- [75] <https://www.linux-nantes.org/>
- [76] <https://www.april.org/>
- [77] <https://www.laquadrature.net/>
- [78] <https://www.amnesty.org/fr/>
- [79] <https://fediverse.party/en/mastodon/>
- [80] https://fr.wikipedia.org/wiki/Internet_Relay_Chat

QUESTIONS / RÉPONSES

MERCI DE VOTRE PARTICIPATION

