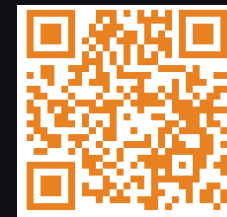
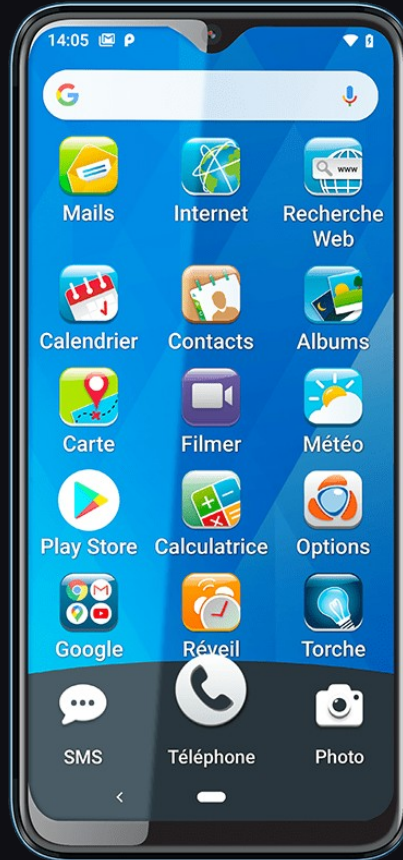


Smartphone et vie privée



Root66.net



Médiathèque d'Élancourt
Intervention : **Benzo**
Association root66.net



Association root66.net

- Depuis 1999
- Les logiciels libres
- Conférences
- Permanences & ateliers
- Install Party & smartphone Party
- Formations



👉 aider à être autonome, à améliorer sa vie privée et sa sécurité

Disclaimer

Ce que sera ou ne sera pas cette conférence :

- ✓ Conférence grand public – accessible – non exhaustive
- ✓ Atelier grand public – théorie à la pratique

Objectif: fournir clés de compréhension

- sur l'enjeu vie privée/smartphone
- sur les solutions pour se protéger

Comprendre et agir !

Smartphone et vie privée

Plan

1 - Smartphone : l'espion qui m'aimait

- C'est quoi un smartphone ?
- Comment on est tracké ?



2 - Comment mieux protéger sa vie privée ?

- Solutions simples et concrètes
- Solutions avancées

intro

Vie privée ?

- - ce qu'on ne veut pas rendre public
- - droit fondamental
- - sondage / test ? volontaire ?
- - « *je n'ai rien à cacher* »
 - Prête moi ton smartphone et laisse moi regarder
 - Toi oui , mais un de tes proches peut-être?
Aujourd'hui oui. Mais demain ?

Le contexte

Les affaires- révélations

- 2013 Révélations Snowden
- 2016 Cambridge Analytica
- 2025 Fuite de données, databrokers files

→ ciblage publicitaire, surveillance de masse, manipulations

Le contexte

Les menaces

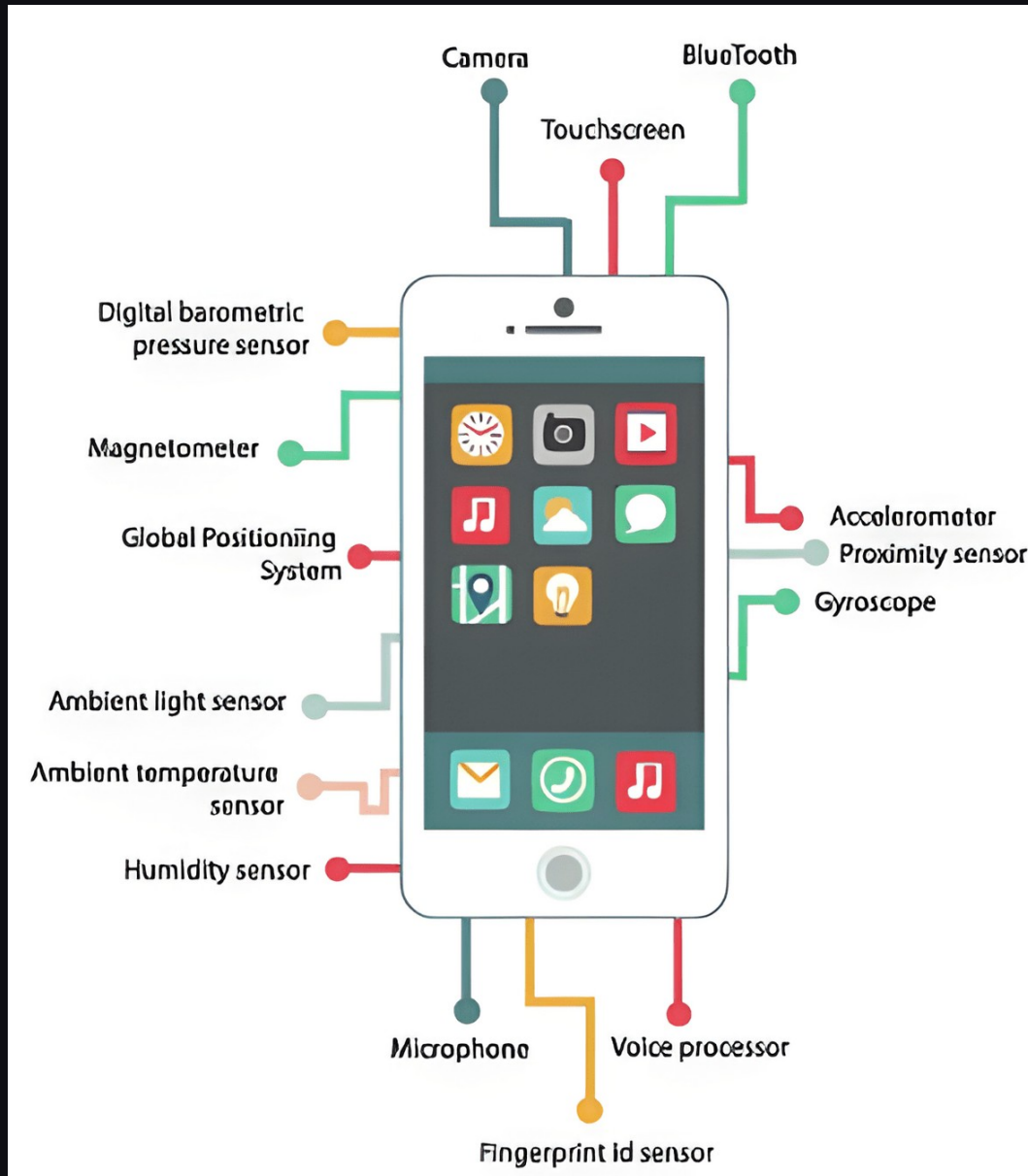
- Les entreprises commerciales / Big Tech
- Les cybercriminels
- L'État - opérateurs telecom
- Tiers proche



Smartphone : définition ?

- Téléphone intelligent ?
- Ordiphone ?
- Photophone ?

C'est quoi smartphone ?



Les traces numériques

Que sait votre smartphone sur vous ?

- où vous allez
- avec qui vous parlez
- ce que vous cherchez
- vos habitudes

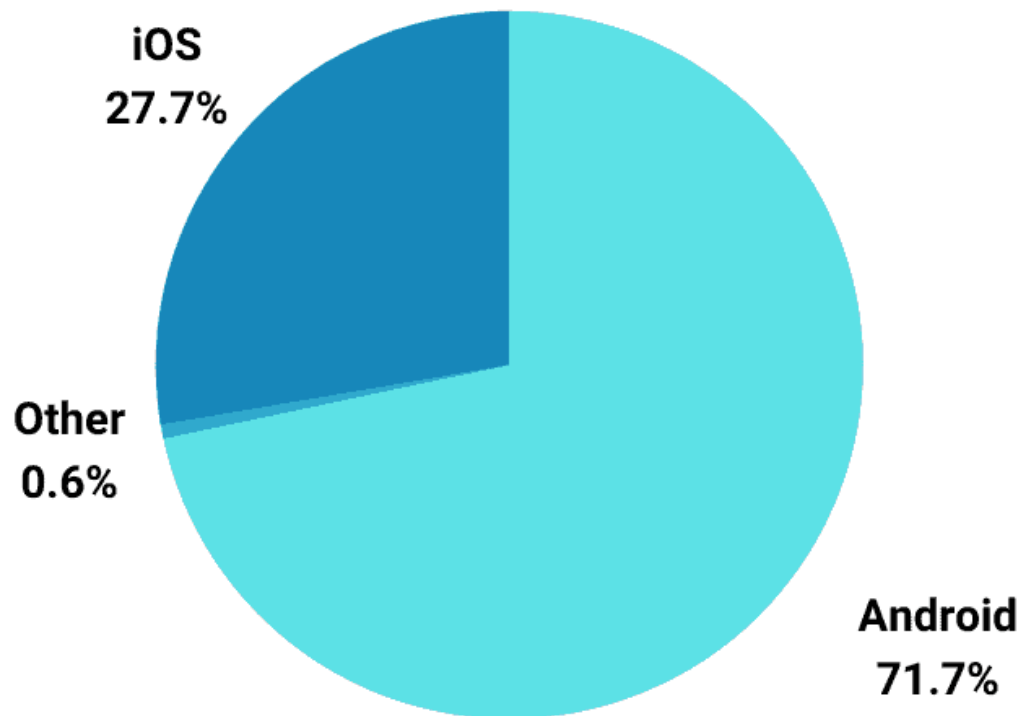
« Doudou espion »
toujours allumé
greffé avec nous partout et tout le temps



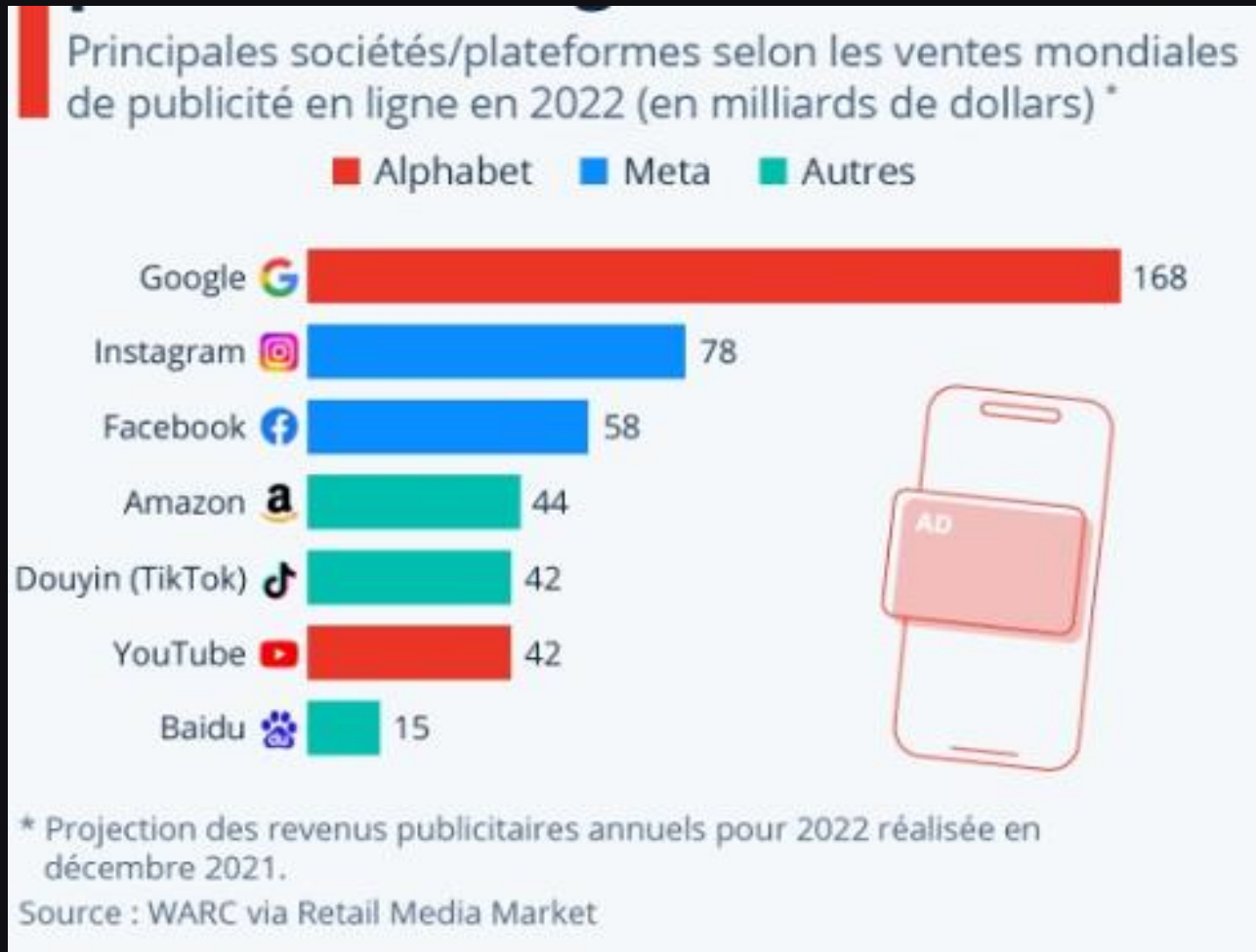
C'est quoi smartphone ?

Quel système d'exploitaton ?

**Android vs. iOS Market Share:
Which Mobile OS Has the Most Users Worldwide?**



C'est quoi Android ?



Google est au cœur du système

C'est quoi Android ?



Comment on est tracké ?

Les google « plaies »



les google play services



le google play store

- **préinstallés**
 - **superprivilèges**
 - **boite noire**, toujours active en arrière plan
 - **tracking silencieux** : sans action ni consentement
- pisteurs installés

Comment on est tracké ?

Quelles données ?

- identifiants techniques :
IMEI , IMSI , MAC,
IP, nom d'hôte...
- **ID publicitaire**
données de géolocalisation
- compte gmail , numero tel
- métadonnées

Comment on est tracké ?

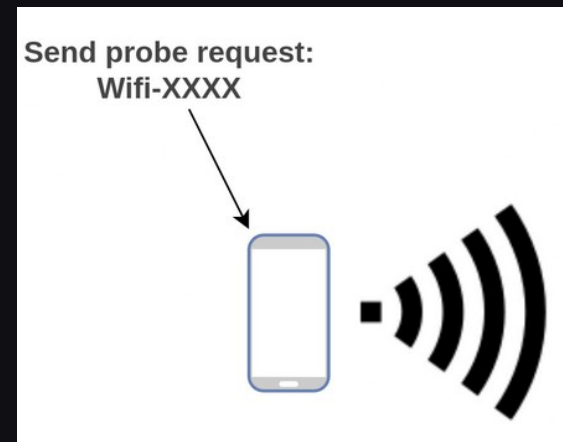
Exemple de tracking : -  En magasin

 Tracking réel utilisé

Ton smartphone cherche en permanence des réseaux : à la maison, dans la rue, dans un magasin 

 pour ça, il envoie des messages dans l'air :

 les probe requests



Comment on est tracké ?

Exemple de tracking : -  En magasin

 Tracking réel utilisé

- Le magasin installe des capteurs Wi-Fi
- Ces capteurs écoutent les probe requests des smartphones

Ils détectent :

- adresse MAC ,
- puissance du signal (distance)
- Fréquence de passage ,
- noms reseaux wifi connus

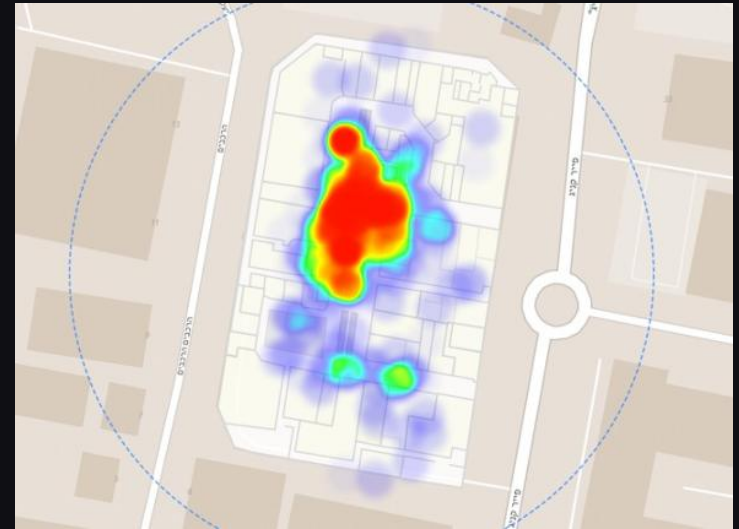
Comment on est tracké ?

- Exemple de tracking : -  En magasin

-  Tracking réel

👉 Résultat:

- parcours client ds le magasin
- temps passé dans un rayon
- nombre de passage clients



Pratique moins utilisée officiellement
→ RGPD et random mac

Quand vous coupez le Wi-Fi, vous coupez Internet...
pas forcément l'antenne !

Comment on est tracké ?



L'empreinte du navigateur

- - technique **fingerprinting** - (user-agent)
- - créer **1 empreinte unique** basée sur :
 - Langue , fuseau horaire
 - Polices de caractère, taille de l'écran
 - Extensions
 - Versions Système d'exploitation et navigateur...



nous rend unique



permet de nous identifier

Les applications

Les GAPPS

Les applications Google machin ...



- Gmail : lit le contenu des mails



- Chrome : Historique de connexion, IP, appareil, localisation



- gogol drive : fichiers activités

- ok google : reconnaissance vocale, écoute en permanence

...

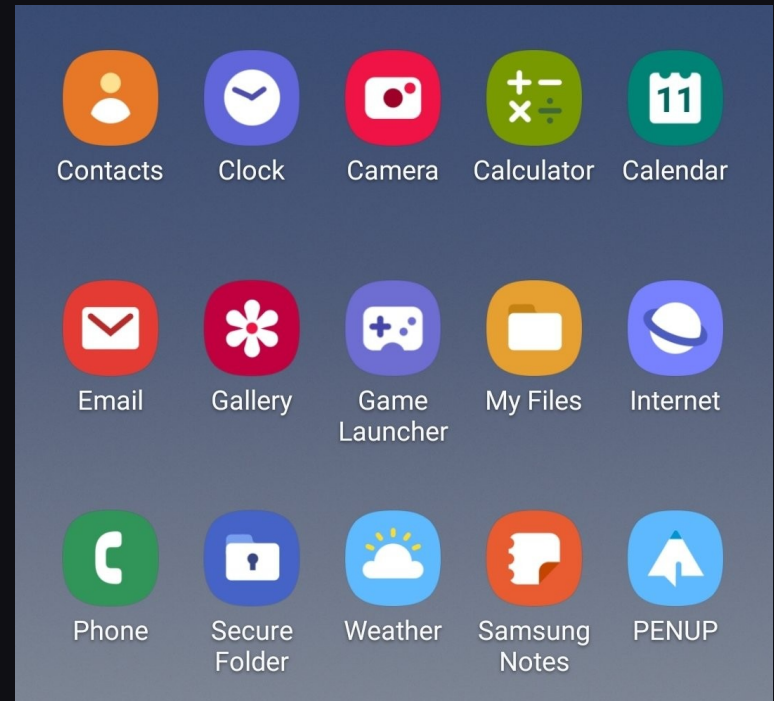
Données stockées hors UE – cloud Act – rgpd partiel
google = régie publicitaire

Les applications

Constructeurs

Xiaomi, Huawei, Oppo...

- explorateur de fichier
- notes
- bureautique
- lecteur video



Préinstallées – difficiles à supprimer

Permissions abusives :

contact , agenda , geoloc etc

Collecte + envoie données hors UE

Les applications

Constructeurs



Mi Browser

11

trackers

82

permissions

Version 14.51.0-gn - [see other versions](#)

Source: Google Play

Report created on Feb. 16, 2026, 9:59 p.m.

[See on Google Play >](#)

Certaines autorisations peuvent se réactiver seules même après désactivation !

Source : <https://reports.exodus-privacy.eu.org/en/reports/com.mi.globalbrowser/latest/>

Les applications

Collecte des données

1) Active : Les données actives = celles liées à ton compte: *recherches, historique YouTube, emails Gmail, calendrier.*

👉 Ces données sont directement associées à ton identité.

2) Passive : en arrière plan
celles collectées indépendamment de ton compte :
IMEI, localisation réseau, identifiants publicitaires, comportement d'utilisation...

👉 Ces données sont collectées même sans compte !!

Le système android

Collecte passive

📶 COLLECTE EN COURS

Ton Android en veille envoie ça à Google

- Localisation — 14x / heure
- Réseaux Wi-Fi à proximité
- Liste de tes applications
- Numéro IMEI + carte SIM
- Check-in système / 40 min

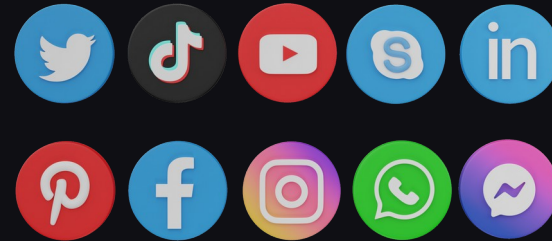
Sans interaction. Sans compte Google.
Même GPS désactivé.

Les applications

Les applications

Les pires applications en matière de tracking :

- réseaux sociaux
- santé / sport
- VPN gratuits
- lampe torche...



▷ Vidéo

Comment le porte-avions "Charles-de-Gaulle" a été localisé en temps réel à cause d'une application de sport

Le porte-avions Charles-de-Gaulle a pu être localisé en temps réel à cause d'un militaire qui a partagé son footing sur l'application de sport Strava.

Comment on est tracké ?

Résumé

Votre smartphone vous suit en permanence

- Même sans action de votre part
- sans consentement réel
- même en veille
- Votre smartphone ne vous appartient pas

Peut-on lutter contre ça ???



Comment reprendre le contrôle ?

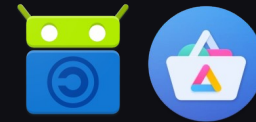
Pour améliorer sa vie privée



Solutions : applications libres

Pour améliorer sa vie privée

- Les magasins (stores) : **Fdroid** et **Aurora**



Critère	F-Droid (libre)	Play Store (classique)
Code source	✓ Ouvert	× Propriétaire
Permissions	Minimales	Souvent excessives
Tracking	× Aucun	✓ Très fréquent
Dépendance Google	×	✓ (Play Services)
Modèle économique	Don / libre	Publicité / data

Les applications

Pour améliorer sa vie privée

Les incontournables :

- **Firefox** + ublock origin



- Mail : **Thunderbird**



- Messagerie chiffrée : **Signal**



- Mots de passe : **Keepass**



- Se déplacer : **Osmand** , **comaps**



- Clavier : **Helliboard**

- youtube : **Newpipe**

- Notes : **Joplin**

- **shelter** : pour cloisonner les apps

Les applications

Conseils + au - simple

- 1 – Ne pas utiliser d'application 🙄
- 2 – Utiliser des applications libres téléchargées sur **Fdroid**
- 3 – Utiliser les **sites web** plutôt que des applis
ex : météo, maps ...
- 4 – Télécharger applications via **Aurora** -mode anonyme
- 5 – Installer les applications dans un profil séparé (**shelter**)

Les applications

Les services en ligne

alternatives aux services les + critiques :

- moteur de recherche : **duckduckgo**, **searX**



- cloud : **Nextcloud**

(synchro fichiers, photos, agenda, contacts)



- mails : **tuta** , **protonmail**

 ProtonMail



- visios : **jitsi**, **big blue button**



jitsi.org



Les services en ligne

Quelles alternatives libres et éthiques ?



LES CHATONS

Les services en ligne

Quelles alternatives libres et éthiques ?



Qézaco ?

Collectif des Hébergeurs Alternatifs, Transparents,
Ouverts, Neutres et Solidaires

Principe des AMAP - Label

Les services en ligne

Quelles alternatives libres et éthiques ?

S'organiser ensemble



Framagenda



Google-Agenda

Choisissez qui verra votre planning.

[Utiliser Framagenda >](#)



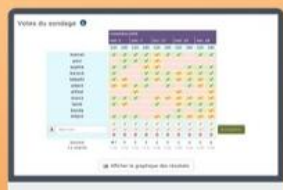
Framacount



Tricount

Gérez facilement vos dépenses partagées.

[Utiliser Framacount >](#)



Framadate



Doodle

Planifiez vos réunions ou prenez des décisions

[Utiliser Framadate >](#)



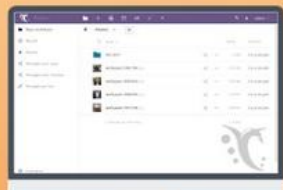
Mobilizon



Facebook-Event

Trouvez, créez et organisez vos événements. Animez vos groupes.

[Utiliser Mobilizon >](#)



Framaspace



Google-Workspace

Cloud convivial pour collectifs solidaires.

[Utiliser Framaspace >](#)



Framavox



Shrtet

Prenez vos décisions ensemble, collaborativement.

[Utiliser Framavox >](#)

Les services en ligne

Qui propose services libres et éthiques ?

Associations et entreprises

- framasoftware.org
- chatons.org

...

Proton

infomaniak

Comment reprendre le contrôle ?

Méthodes pour limiter le pistage

Configurer :

- 1 - **compte google (= bof !)** 😞
- 2 - **paramètres systèmes** 😎
 - extinction auto : Bluetooth, wifi
 - **config wifi**
 - **dns** (souvent oublié- gros enjeux)
 - **clavier**
- 3 - **applications** : applications libres 😊
- 4 - **services en ligne** : libres et éthiques 😊

Comment reprendre le contrôle ?

Méthodes pour limiter le pistage

Configurer :

- 1 - **compte google** (= bof !)
- 2 - **paramètres systèmes**
 - extinction auto : Bluetooth, wifi
 - **config wifi**
 - **dns** (souvent oublié- gros enjeux)
 - **clavier**
- 3 - **applications** : applications libres
- 4 - **services en ligne** : libres et éthiques

Comment reprendre le contrôle ?

L'hygiène numérique

Comme se laver les mains

→ des gestes simples et réguliers,
pas besoin d'être expert



Les risques sont invisibles

→ on prévient plutôt que subir (virus, arnaques...)

Tout le monde est concerné

→ chacun peut adopter de **bonnes habitudes, pratiques**

Comment reprendre le contrôle ?

Les 10 commandements



10 COMMANDEMENTS DU SMARTPHONE

1. Tu utiliseras des logiciels libres



2. Tu protégeras l'accès à ton téléphone



3. Tu ne connecteras pas ton smartphone n'importe où



4. Tu te méfieras des messages suspects



5. Tu mettras à jour régulièrement



6. Tu installeras des applis avec prudence



7. Tu contrôleras les autorisations des apps



8. Tu sécuriseras tes connexions



9. Tu protégeras tes comptes



10. Tu protégeras tes données (sauvegardes)

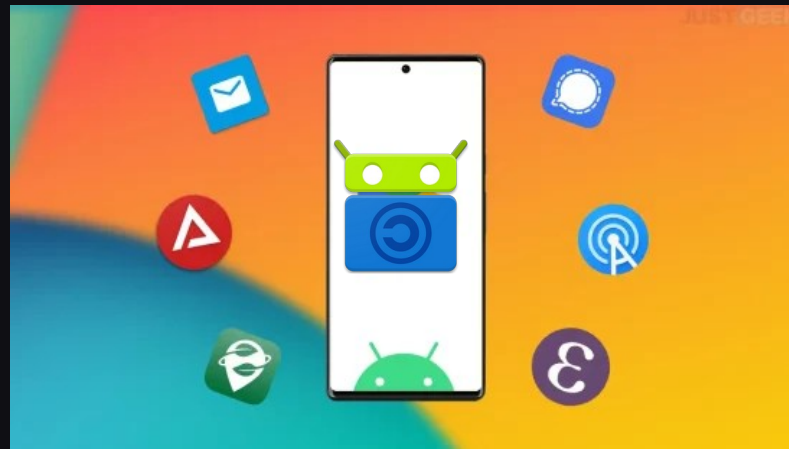


Comment reprendre le contrôle ?

Règle n°1

🔑 Tu utiliseras des logiciels libres

- sécurité
- vie privée
- confiance



Comment reprendre le contrôle ?


Règle n°2

Tu protégeras ton téléphone

- Code PIN long ou mot de passe
- Verrouillage automatique rapide
- Évite les schémas
- Utilise un filtre de confidentialité
- Ne le prête à personne

Comment reprendre le contrôle ?

Règle n°3

2.  Tu ne connecteras pas ton smartphone n'importe où

- Évite les ports USB publics (gare, borne de recharge...)
- N'utilise pas d'ordinateur inconnu

Risque : “juice jacking” (vol de données / infection)

 Privilégie ton chargeur et une prise secteur

Comment reprendre le contrôle ?

Règle n°4

✉ Tu te méfieras des messages suspects

- SMS, mails, messageries inconnues
- Ne clique pas sur les liens douteux
- Ne flashe pas des qr codes

Méfiez-vous de cette arnaque sur les bornes de recharge

Mieux vaut prévenir que guérir

🕒 3 min



Raphaëlle Baut



Comment reprendre le contrôle ?

Règle n°5

 Tu mettras à jour régulièrement

- Système (Android / iOS)
- Applications

Comment reprendre le contrôle ?

Règle n°6



Tu installeras des applis avec prudence


- Uniquement si besoin via **Fdroid** ou Aurora (Google Play Store en mode anonyme)
- Vérifie les avis , l'éditeur et les permissions
- Supprime les applis inutiles

Comment reprendre le contrôle ?

Règle n°7

 Tu contrôleras les autorisations des apps

- Caméra
- micro
- localisation
- contact

 Refuse ce qui n'est pas nécessaire

Comment reprendre le contrôle ?

Règle n°8



Tu sécuriseras tes connexions

- Évite les Wi-Fi publics ouverts
- Coupe Bluetooth / Wi-Fi / 4g si inutiles
- utilise messageries sécurisées (E2E)
- Utilise un VPN si t'as pas confiance

Utilise le Chiffrement de bout en bout

Comment reprendre le contrôle ?

Règle n°9

Tu protégeras tes comptes

- Mot de passe unique et complexe
- Gestionnaire (ex : keepass)
- Active la double authentification - MFA

Comment reprendre le contrôle ?

Règle n°10

Tu protégeras tes données (sauvegardes)


- Sauvegardes régulières
- Anticiper perte, vol ou piratage

Sinon ...
c'est le drame !



Les solutions

Smartphones dégooglisés

OS	Logiciel libre	Pays / origine	Modèle économique	Objectif principal	Sécurité	Compatibilité
LineageOS	● Majoritairement libre	 (communauté)	Bénévolat / dons	Customisation	★★☆☆☆	★★★★★★
GrapheneOS	● Libre + composants propriétaires Android		Dons + sponsors	Sécurité maximale	★★★★★★	★★☆☆☆
CalyxOS	● Libre (avec microG)	 (Calyx Institute)	ONG / dons	Vie privée accessible	★★★★★☆☆	★★☆☆☆☆
iodéOS	● Libre + services propriétaires iodé		Freemium (services payants)	Vie privée + anti-pub	★★★★☆☆☆	★★★★★★☆
/e/OS	● Libre + services dégooglisés (microG)	 (Murena)	Vente d'appareils + services cloud	Vie privée grand public (sans Google)	★★★★☆☆☆	★★★★★★☆
Replicant	● 100% libre (FOSS strict)	 (communauté FSF) ↓	Bénévolat / dons	Pureté logicielle	★★★★★☆☆	★☆☆☆☆

Les solutions

Smartphones dégooglisés

murena.com/fr/

Boutique Smartphones Workspace Enfants Pour les Entreprises À propos

murena

FR

Dites NON au Big-Tech ! La liberté commence par la protection de la vie privée.

Protégez votre liberté et la vie privée de votre famille avec les smartphones Murena

J'en profite

Découvrez Murena Workspace

fairphone

Les solutions

Les smartphone party 🎉

Smartphone Party: root66 t'aide à libérer ton smartphone des Gafam !



Root66 organise une **smartphone Party** le samedi 21 juin à 14h à [St Cyr L'Ecole](#).

Le smartphone est notre meilleur compagnon .Il ne nous quitte jamais, mais il est aussi notre meilleur espion.

Dès lors comment faire pour limiter la collecte de nos données personnelles et protéger notre vie privée ?

Sources

- 1) *Espionné par nos apps :*
<https://www.arte.tv/fr/videos/123951-000-A/espionnes-par-nos-apps/>
- 2) *Data Brokers Files : tout ce que les données disent de vous*
<https://www.radiofrance.fr/franceculture/podcasts/recits-d-enquete/recits-d-enquete-chronique-du-samedi-15-fevrier-2025-2993359>
- 3) *Google collecte sur un android :*
<https://webologie.me/google-collecte-android>
- 4) *Whatsapp danger*
<https://tutox.fr/2026/02/27/whatsapp-chez-les-militants-coup-de-gueule/>
- 5) *Tracking indoor*
[:https://www.mocapplatform.com/blog/dynamic-heatmap-for-indoor-location-analytics](https://www.mocapplatform.com/blog/dynamic-heatmap-for-indoor-location-analytics)
- 6) *Associations libération smartphones :*

<https://www.electrocycle.co/>
<https://root66.net>
- 7) *Acheter un smartphone degooglisé*
<https://murena.com/fr/>
- 8) *Installer GrapheneOS , un des meilleurs android sécurisés*
<https://grapheneos.org>

Questions ?

