Fiche Pratique N°52 : Réglez la confidentialité de votre téléphone V1.2

7 nov, 2026 · @Gabriel

Objectif : *reprendre la main sur ce que votre téléphone et ses applications collectent (position, micro, contacts, identifiant publicitaire), sans changer de téléphone ni installer quoi que ce soit, en attendant, si vous le souhaitez, de passer à un téléphone sans Google (fiche N°64).*

- ***Public visé :*** *débutant*
- ***Temps estimé :*** *20 à 30 minutes*
- ***Difficulté :*** ★☆☆☆☆ *(Très facile)*
- ***Concerne :*** *Android et iPhone (les intitulés varient un peu selon la marque et la version)*
- ***Fiches associées :*** *N°2 (navigateur), N°17 (moteur de recherche), N°18 (double authentification), N°42 (Aurora Store), N°19d et N°19e (sauvegardes locales), N°24 (cartes), N°46 (gestes de base), N°48 (outils de cybersécurité), N°57 (clavier), N°64 (téléphone sans Google)*

1. Pourquoi régler son téléphone ? (Le problème)

Le téléphone est l'objet le plus personnel que nous possédons : il sait où nous dormons, qui nous appelons, ce que nous photographions. Chaque application peut demander l'accès à une partie de ces informations, et beaucoup en demandent plus qu'elles n'en ont besoin.

Ce que le téléphone peut révéler	Exemple
Votre position en continu	Domicile, travail, médecin, lieu de culte
Vos contacts	Le carnet d'adresses de vos proches, sans leur accord
Vos photos	Avec la date et le lieu de prise de vue
Votre micro et votre caméra	Une application de lampe torche n'en a aucun besoin
Votre identifiant publicitaire	Un numéro qui relie votre activité d'une application à l'autre

Une image pour comprendre : votre téléphone est une maison. Chaque application est un invité à qui vous prêtez des clés. Ce réglage consiste à revoir qui a les clés de quelle pièce, et à reprendre celles qui ne servent à rien.

Le risque : des données très personnelles, les vôtres et celles de vos proches, revendues pour la publicité.

Le bénéfice : en vingt minutes, la plupart des fuites sont fermées. Et souvent, la batterie dure plus longtemps.

2. Les 8 réglages essentiels

#	Réglage	Android	iPhone
1	Revoir les autorisations	Paramètres › Sécurité et confidentialité › Confidentialité › Gestionnaire d'autorisations	Réglages › Confidentialité et sécurité

gabriel.ananda@mailo.com
CC BY SA

#	Réglage	Android	iPhone
2	Localisation « seulement pendant l'utilisation »	Paramètres › Localisation › Autorisations des applications	Réglages › Confidentialité et sécurité › Service de localisation
3	Position approximative plutôt qu'exacte	Dans l'autorisation de chaque application : décocher « Utiliser la position exacte »	Dans chaque application : désactiver « Position exacte »
4	Couper l'identifiant publicitaire	Paramètres › Confidentialité (ou Sécurité et confidentialité › Autres paramètres de confidentialité) › Annonces › Supprimer l'identifiant publicitaire	Réglages › Confidentialité et sécurité › Suivi : désactiver « Autoriser les demandes de suivi »
5	Publicités personnalisées	myadcenter.google.com (Mon Centre publicités) : désactiver les annonces personnalisées	Réglages › Confidentialité et sécurité › Publicité Apple : désactiver « Publicités personnalisées »
6	Envoi de statistiques au fabricant	Paramètres › Google › Utilisation et diagnostics : désactiver	Réglages › Confidentialité et sécurité › Analyses et améliorations : désactiver
7	Supprimer les applications inutilisées	Laisser activée la réinitialisation automatique des autorisations des applis inutilisées, puis désinstaller	Réglages › Général › Stockage de l'iPhone
8	Vérifier qui a accès à quoi	Tableau de bord Confidentialité (dans Paramètres › Sécurité et confidentialité)	Rapport de confidentialité des apps, et Contrôle de sécurité

Les noms exacts varient selon la marque (Samsung, Xiaomi, Pixel…) et la version. Si vous ne trouvez pas un menu, tapez son nom dans la loupe en haut des Paramètres ou des Réglages.

3. Revoir les autorisations, application par application

La bonne question pour chaque autorisation : **cette application en a-t-elle vraiment besoin pour me rendre service ?**

1. Ouvrez le gestionnaire d'autorisations (réglage 1 du tableau).
2. Commencez par **Position**, puis **Micro**, **Appareil photo**, **Contacts**, **Photos et vidéos**.
3. Pour chaque application de la liste, choisissez :
    - **« Refuser »** si elle n'en a pas besoin (un jeu n'a pas besoin de vos contacts) ;
    - **« Seulement pendant l'utilisation »** si elle en a besoin de temps en temps (une application de cartes) ;
    - **« Demander à chaque fois »** en cas de doute.

gabriel.ananda@mailo.com
CC BY SA

- **Vous devez voir :** la liste « Autorisée en permanence » presque vide.

4. Pour les photos, choisissez « Accès limité » (ou « Photos sélectionnées ») plutôt que toute la galerie.

Application	Autorisations raisonnables
Cartes, GPS	Position pendant l'utilisation
Messagerie	Contacts, micro, appareil photo
Banque	Appareil photo (pour scanner un chèque), rien d'autre
Lampe torche, calculatrice, jeux	Aucune
Météo	Position approximative, ou aucune si vous choisissez la ville à la main

4. Localisation : le réglage le plus important

- Passez toutes les applications en **« Seulement pendant l'utilisation »** ou **« Jamais »**.
- Donnez la **position approximative** aux applications qui n'ont pas besoin de savoir dans quelle rue vous êtes (météo, actualités).
- Sur iPhone, regardez aussi **Service de localisation › Services système › Lieux importants** : c'est l'historique de vos lieux fréquents. Vous pouvez l'effacer et le désactiver.
- Sur Android, l'historique de vos trajets (la **Chronologie** de Google Maps, anciennement Historique des positions) est désormais stocké sur le téléphone. Dans Google Maps, touchez le point bleu de votre position pour voir s'il est activé, puis désactivez-le ou réglez sa suppression automatique.

5. Publicité et suivi entre applications

- **Android :** supprimez l'identifiant publicitaire (réglage 4). Le téléphone ne transmet plus ce numéro qui permet de vous reconnaître d'une application à l'autre.
- **iPhone :** désactivez « Autoriser les demandes de suivi » : les applications ne peuvent plus même poser la question, et la réponse est « non » pour toutes.
- Partout : désactivez les **publicités personnalisées** et l'envoi de **statistiques** (réglages 5 et 6).

6. Comptes, sauvegardes et applications

- **Faites le ménage :** une application désinstallée ne collecte plus rien. Supprimez celles que vous n'avez pas ouvertes depuis trois mois.
- **Remplacez les applications des géants par des alternatives libres :** navigateur (fiche N°2), moteur de recherche (fiche N°17), cartes (fiche N°24), clavier (fiche N°57). Sur Android, désactivez celles de Google que vous ne pouvez pas désinstaller (Paramètres › Applications › l'application › Désactiver).

gabriel.ananda@mailo.com
CC BY SA

- **Sauvegardes dans le cloud :** la sauvegarde automatique envoie vos contacts, messages et photos chez Google (Google One) ou Apple (iCloud). Préférez une sauvegarde locale sur ordinateur ou disque (fiches N°19d et N°19e), puis désactivez la sauvegarde dans le cloud.
- **Installez depuis les sources officielles :** Play Store, App Store, ou Aurora Store et F-Droid sur Android (fiche N°42). Jamais un fichier .apk reçu par message.
- **Mettez à jour** le système et les applications : la plupart des mises à jour corrigent des failles de sécurité.
- **Verrouillez :** un code à 6 chiffres au minimum, et un verrouillage automatique après 1 minute.
- **Notifications sur l'écran verrouillé :** masquez leur contenu, pour que vos messages et codes de connexion ne s'affichent pas à la vue de tous.

7. Savoir ce que font vos applications

Sur Android : Exodus Privacy. Exodus Privacy est une association française qui analyse les applications Android et liste les traqueurs qu'elles contiennent.

1. Installez l'application **Exodus Privacy** depuis F-Droid ou le Play Store.
2. Ouvrez-la : elle affiche vos applications installées, avec pour chacune le nombre de **traqueurs** et d'**autorisations**.
    - **Vous devez voir :** un nombre en couleur à côté de chaque application ; 0 traqueur, c'est l'idéal.
3. Touchez une application pour voir le détail des traqueurs (publicité, statistiques, localisation).
4. Pour une application que vous n'avez pas encore installée, consultez son rapport sur **reports.exodus-privacy.eu.org** avant de l'installer.

Exodus ne bloque rien : il vous informe pour que vous choisissiez une alternative plus sobre.

Sur iPhone : le rapport de confidentialité des apps. Réglages › Confidentialité et sécurité › **Rapport de confidentialité des apps** : activez-le, puis revenez une semaine plus tard. Il montre quelles applications ont utilisé votre position, votre micro ou vos contacts, et quels domaines elles ont contactés. Dans l'App Store, la rubrique **« Confidentialité de l'app »** de chaque application liste les données qu'elle collecte.

Partout : les voyants. Un point vert ou orange en haut de l'écran signale que la caméra ou le micro est en cours d'utilisation. S'il apparaît sans raison, vérifiez quelle application l'utilise.

Pour aller plus loin : ces réglages limitent la collecte, mais Android garde des services Google intégrés au système, et l'iPhone vous lie à votre compte Apple. Pour supprimer la collecte à la source, passez à un système sans Google comme /e/OS ou GrapheneOS (fiche N°64).

8. À savoir avant de se lancer

Crainte fréquente	La réalité
« Mes applications ne vont plus marcher. »	Si une application a vraiment besoin d'une autorisation, elle vous la redemandera au moment voulu.
« Je vais tout dérégler. »	Chaque réglage se remet en place en un geste. Rien n'est définitif.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°52 : Réglez la confidentialité de votre téléphone V1.2

Crainte fréquente	La réalité
« Je n'ai rien à cacher. »	Il ne s'agit pas de cacher, mais de choisir : vos déplacements et le carnet d'adresses de vos proches ne regardent pas les annonceurs.
« Mon téléphone n'a pas ces menus. »	Les noms varient selon la marque : utilisez la loupe des Paramètres.
« Il faudrait changer de téléphone. »	Non : ces réglages sont le premier pas, sur le téléphone que vous avez.

9. Challenge 7 jours

- **Jour 1 :** revoir les autorisations de **position**.
- **Jour 2 :** revoir **micro** et **appareil photo**.
- **Jour 3 :** revoir **contacts** et **photos**.
- **Jour 4 :** couper l'identifiant publicitaire et les publicités personnalisées.
- **Jour 5 :** désinstaller 5 applications inutilisées.
- **Jour 6 :** consulter Exodus Privacy ou le rapport de confidentialité des apps.
- **Jour 7 :** remplacer l'application la plus gourmande par une alternative plus sobre.

10. En résumé (ce que vous gagnez)

Action	Bénéfice
Autorisations au plus juste	Chaque application n'a que les clés dont elle a besoin
Localisation maîtrisée	Vos déplacements ne sont plus enregistrés en continu
Identifiant publicitaire coupé	Plus de suivi d'une application à l'autre
Ménage des applications	Moins de collecte, plus de place, plus de batterie
Exodus Privacy ou rapport iPhone	Vous savez qui collecte quoi

11. À retenir absolument

- **Une autorisation, une question :** l'application en a-t-elle vraiment besoin ?
- **Localisation :** « seulement pendant l'utilisation », et approximative quand c'est possible.
- **Identifiant publicitaire :** supprimé sur Android, suivi refusé sur iPhone.
- Moins d'applications = moins de collecte ; et des applications libres plutôt que celles des géants.
- **Tout est réversible :** on peut régler sans crainte.

Test final : ouvrez le tableau de bord Confidentialité (Android) ou le rapport de confidentialité des apps (iPhone). Si aucune application inattendue n'a utilisé votre position ou votre micro ces derniers jours, vous avez réussi ✅

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°52 : Réglez la confidentialité de votre téléphone V1.2

Références

- Android – votre confidentialité, vos choix
- Google – technologies publicitaires et identifiant publicitaire
- Apple – contrôle de la confidentialité
- Apple – contrôler les publicités personnalisées
- Apple – confidentialité et service de localisation
- Digitec – la Chronologie de Google Maps stockée en local (2025)
- iPhon.fr – 12 réglages de sécurité et de confidentialité
- Exodus Privacy
- Exodus Privacy – rapports par application
- Exodus Privacy – Exodus sur F-Droid

gabriel.ananda@mailo.com
CC BY SA