[Fiche 13] Les ordiphones

Des ordinateurs de poches accompagnent une grande majorité d'entre nous. Ces ordiphones (ou *smartphones*) sont devenus des interfaces pour de nombreux usages du quotidien. Pourtant, ces couteaux suisses numériques constituent souvent une faille importante pour la sécurisation des données et la protection des libertés. Conçus pour communiquer, ils intègrent de nombreux capteurs chargés, en permanence, d'analyser (et de quantifier) l'environnement de l'appareil : détection et connexion à de nombreux réseaux, capteurs visuels (photo et vidéo), microphone, géolocalisation, position spatiale (accéléromètre), etc.
Ces petits ordinateurs sont plus difficilement contrôlables que leurs ainés : ils sont rarement "non connectés", les composants sont souvent plus spécifiques et les constructeurs exercent un pouvoir plus élevé sur ces matériels. La contrainte la plus conséquente vient des fournisseurs du système d'exploitation. Il s'agit d'un secteur duopolistique où Google et Apple sont très largement majoritaires et imposent, par défaut, un compte connecté chez eux pour utiliser l'appareil ainsi que des logiciels de bases souvent impossibles à supprimer. Cette dépendance à ces deux acteurs dont les atteintes aux libertés sont fréquemment dénoncées pose problème et il est difficile de trouver ou mettre en place des alternatives éthiques. Il faut donc acter qu'il existe un problème intrinsèque des ordiphones en matière de respect des libertés.
Des méthodes simples permettent néanmoins de limiter les dégâts face à d'autres atteintes possibles. Comme pour un ordinateur classique, il existe des applications et des bonnes pratiques permettant de mieux protéger ses données : utiliser des phrases de passe, chiffrer ses données et ses communications, se renseigner sur les services que l'on utilise et opter pour des services respectueux des libertés, utiliser des applications libres, etc. De plus, des projets d'ordiphones "libérés" et systèmes d'exploitation plus éthiques se développent.

Quelques bonnes pratiques de paramétrage

Les ordiphones peuvent facilement être volés, perdus ou victimes d'applications malveillantes. Adopter de bonnes pratiques, activer des paramètres de sécurité et chiffrer ses données vont assurer une première couche de protection.

- **Minimiser les données stockées** : face à la vulnérabilité de tels appareils, mieux vaut limiter les données qui y sont stockées et ne pas y conserver de données sensibles telles que des coordonnées bancaires, des mots de passe, des codes d'accès, des informations médicales, etc.
- **Activer le code PIN** : il sera demandé à chaque allumage et constitue une mesure basique. Il ne protège que l'accès aux réseaux de communication de l'opérateur *via* la carte SIM. Attention : sans autre mesure de protection, les données de l'appareil resteront accessibles et celui-ci pourra toujours être connecté en Wifi. Il est également important de remplacer le code par défaut (0000, 1234…)
- **Conserver son code IMEI** : c'est le numéro de série de chaque ordiphone. En cas de vol, il permet de bloquer l'usage du téléphone sur tous les réseaux. Il est possible de l'obtenir en tapant *#06# sur le clavier du téléphone.
- **Verrouillage de l'appareil** : à chaque extinction de l'écran, un code d'accès est demandé pour déverrouiller l'ordiphone. Il s'agit de sécuriser l'accès rapide à l'appareil. Sans ce code, impossible d'utiliser directement l'ordiphone, couplé au chiffrement des données cela limite grandement les accès aux données en cas d'accès illégitime à l'appareil. Le verrouillage s'active facilement dans les paramètres de sécurité. Il est préférable de privilégier un code plutôt qu'un schéma, facile à observer, ou des données biométriques.

- **Maitriser ses capteurs** : les ordiphones disposent de nombreux capteurs. Il est possible d'en rendre certains inactifs en les paramétrant. Il est ainsi conseillé de les désactiver dès qu'ils ne sont plus utilisés. Il s'agit surtout de la **localisation GPS** qui peut être utilisée et récupérée par de nombreuses applications même en apparence inactives, mais aussi de la connexion Bluetooth, ou même Wifi et réseaux mobiles (qui permettent potentiellement de tracer les positions et les lieux visités). Dans les périodes où la connexion n'est pas nécessaire, il ne faut pas hésiter à passer son téléphone en mode « avion » pour limiter les données de connexions. Il est important de désactiver ces connexions dès qu'elles ne sont plus nécessaires et de minimiser la production de données exploitables. Cela ne doit toutefois pas faire oublier l'impossibilité d'un contrôle complet par l'individu : les ordiphones peuvent être utilisés comme des mouchards de poche.
- **Vérifier et maitriser ses paramétrages** : si par défaut un grand nombre d'informations sont transmises aux entreprises « présentes » sur les appareils (Apple, Google, constructeurs, applications…), certains paramétrages permettent de limiter cela. Il est possible de désactiver les « statistiques d'utilisation », mais aussi la fonction « Ok Google ».

  Cette fonction est cachée dans les paramètres, langue et saisie, Saisie Vocale, reconn. Google de Base, roue paramètre, Détecter « Ok Google » et tout désactiver.

D'autres paramétrages peuvent s'avérer pertinents : créer un compte invité, indiquer un contact sur son écran de « verrouillage » dans le cas où l'ordiphone serait perdu et pourrait être retourné, etc. Il est vivement conseillé de prendre le temps de les explorer pour mieux maitriser son appareil.

- **Chiffrer les données stockées** : sur les versions les plus récentes des systèmes d'exploitation mobiles, cette option est simple à activer et ne demande aucune compétence particulière.

  Sur Android, il suffit d'aller dans les paramètres. Puis « sécurité » et d'appuyer sur « chiffrer le téléphone ». L'opération est irréversible et demande un peu de temps. À chaque démarrage, le code sera demandé pour déchiffrer l'appareil ainsi qu'au déverrouillage si l'option est activée.

  Sur iOS, le chiffrement est désormais activé par défaut et il suffit de configurer un mot de passe, dans « Paramètres généraux » et sélectionner « Mot de Passe » ou « Code d'Accès… » pour activer la protection.

- **Contrôler les autorisations de ses applications** : sur les versions les plus récentes des systèmes d'exploitation mobiles, il est possible de contrôler les permissions des différentes applications présentes sur son téléphone et de désactiver celles qui sembleraient problématiques.

  Sur Android 6.0 et +, il faut aller dans « Paramètres », « Applications », cliquer sur la roue dentée puis sur « Autoris. des applis ».
  Sur iOS, le système est différent. Pour activer certaines permissions un accord est demandé, il reste possible ensuite de consulter les applications séparément pour désactiver les permissions jugées non pertinentes ou de consulter globalement celles-ci en allant dans « Paramètres », « Vie privée ».

À noter que pour Android, l'association « Exodus Privacy », Exodus-privacy.eu.org offre une analyse des permissions demandées par les différentes applications ainsi que des empreintes des traqueurs contenus dans ces applications révélant l'ampleur de la surveillance sur ces applications. Une application « Exodus Privacy » pour mobile devrait voir le jour, mais le site Internet constitue déjà un formidable outil pour découvrir ces traqueurs et faire le tri dans ses applications.

Des applications libres plus respectueuses des libertés

Sur ordiphone, toutes les applications ne se valent pas et les conseils précédemment donnés continuent de s'appliquer : privilégier des applications libres et éthiques et limiter le nombre d'entre elles au strict nécessaire. Malgré les incitations à installer des applications dédiées, il est souvent préférable de se contenter de la page web mobile du service souhaité pour limiter les traqueurs et l'usage des ressources de l'appareil.

F-Droid

Sur les systèmes types « Android », il existe une application regroupant les applications libres : F-Droid.
C'est l'équivalent d'un « magasin d'applications » qui répertorie les applications libres et facilite leurs installations et mises à jour.

Pour l'installer :

> Sur le navigateur de son ordiphone, se rendre sur le site de « F-Droid », https://f-droid.org et cliquer sur « Télécharger F-Droid », cela récupérera l'APK (fichier exécutable de l'application permettant de l'installer) qui devra être lancé pour installer F-Droid. Il faudra peut-être pour cela accepter les « applications provenant de sources inconnues ».

Une fois installé, F-Droid vous permettra d'accéder facilement à certaines des applications citées ici et de les installer et mettre à jour. Attention, d'autres ne seront présentes que sur Google Play (ou directement en APK sur Internet). Les concepteurs de F-Droid sont assez exigeants sur les engagements sur le logiciel libre et l'absence de traqueurs, des exceptions sont tolérées selon les cas, mais toujours mentionnées en tant « qu'antifonctionnalités » (publicités, recours à des éléments annexes non libres…) et il est préférable de bien lire la fiche de chaque application.
Par exemple, pour installer « Silence » (application conseillée plus loin) :

> Lancer F-Droid, Appuyer sur la loupe, Taper « Silence » puis cliquer sur installer à côté de Silence.

Il n'existe pas pour le moment d'équivalent sur iOS, où certaines applications demeurent néanmoins libres (il en va de même sur Google Play).

Les applications de base

Une fois cela fait, les conseils applicables aux ordinateurs s'appliquent à nouveau :

- Installer Firefox en remplacement du navigateur par défaut. Pour cela, il suffit d'aller sur Google Play ou l'AppStore d'Apple et de l'installer Firefox. Il est ensuite possible de l'utiliser par défaut et d'y adjoindre les modules de protection souhaités (notamment uBlock Origin et Decentraleyes) en passant par l'ajout de modules complémentaires au sein de Firefox.
- Il existe également « Firefox Klar ou Focus » conçu pour réaliser des navigations uniques et va isoler la plupart des informations pour limiter le traçage.
- On peut alors changer de moteur de recherche (Qwant, Startpage, Searx…) en allant sur la page du moteur de recherche souhaité et en restant appuyant longuement sur le champ de recherche pour l'ajouter puis le sélectionner par défaut dans les paramètres de recherche.

Le CECIL recommande par ailleurs quelques applications pour des usages fréquents sur mobile :

- **OsmAnd~** disponible sur F-Droid, qui offre un service de localisation et navigation GPS s'appuyant sur les cartes libres d'OpenStreetMap. Il faudra ensuite télécharger les cartes pertinentes à partir de l'interface de l'application (qui resteront accessibles même sans réseau) ;
- **K-9 Mail**, comme application de gestion de courriel pour ordiphone qui permet d'ajouter et de gérer ses comptes. Il faut également noter que Protonmail dispose d'une application dédiée.
- **Twidere** pour utiliser des comptes Mastodon et Twitter ;
- **Nextcloud** pour synchroniser des données en ligne sur un serveur de confiance (par exemple celui de La Mère Zaclys ainsi que DAVDroid qui est un outil de synchronisation de ses contacts et de son agenda complémentaire à une solution Nextcloud ;
- Il est également possible d'utiliser le réseau TOR sur Android par la combinaison de deux applications développées par le Guardian Project : **Orbot** et **Orfox** disponible sur F-Droid. Sur iOS, il existe aussi une application qui n'est toutefois pas officiellement reconnue par le Projet TOR et qui présente certaines limitations imposées par Apple : « Onion Browser ».

Des applications de chiffrement de bout en bout des communications

Comme pour Internet, les téléphones ont été principalement conçus pour faciliter les communications, les problématiques de sécurisation et de protection des correspondances ne sont venues qu'ensuite. De ce fait, les communications échangées classiquement par téléphone peuvent potentiellement être interceptées (selon les cas plus ou moins facilement) ou récupérées par les opérateurs ou les services de renseignement.
Pour remédier à ce problème, des applications ont été développées pour retrouver une certaine protection de ses communications en ligne.

Il n'existe pas de solution parfaitement libre, décentralisée, fonctionnelle, multiplateforme, interopérable, sans aucun défaut éthique, etc. Le CECIL recommande toutefois deux solutions qui permettent de facilement améliorer la sécurité de ses communications en mettant en place un chiffrement de bout-en-bout géré automatiquement par l'appareil et protégeant donc le contenu des échanges sur le réseau.

Signal, pour chiffrer ses appels et ses messages textes

Signal est une application disponible sur iOS et Android qui permet de chiffrer de bout-en-bout et par défaut les communications qui transitent par l'application. Elle assure alors la protection des discussions téléphoniques ou textuelles. Ce logiciel libre est développé par la société Open Whisper Systems qui est principalement financée par des subventions et des dons. Elle a mis en place un protocole de chiffrement des communications par Internet mis en œuvre dans l'application Signal.
L'application est gratuite et s'installe facilement. C'est une application de messagerie texte très commune en apparence où le chiffrement est géré sur l'ordiphone de la personne sans aucune complexité. L'application dispose même d'une interface pour ordinateur qui impose toutefois d'avoir Chrome (le navigateur de Google).
Une autre limite à cette application est qu'elle doit être liée à un numéro de téléphone dont on doit garder le contrôle et qui sera publiquement diffusé. C'est pour le moment justifié par la nécessité de savoir lesquels de ses contacts utilisent également Signal pour échanger avec eux de façon chiffrée. Signal refuse par ailleurs de permettre une interopérabilité avec d'autres clients de

messagerie.

Silence, pour chiffrer ses SMS

Silence est une application libre de chiffrement issue d'un fork du logiciel TextSecure disponible uniquement pour OS type Android.
Silence permet d'échanger des SMS chiffrés sans requérir de réseau Internet. Il ne requiert pas non plus de devoir déclarer son numéro.

> Une fois installé, il suffit de réaliser un échange de clés (conservées sur l'appareil) par un simple clic sur une icône de cadenas ouvert au sein d'une discussion avec une autre personne disposant de Silence.

L'application permet aussi d'échanger des SMS non chiffrés avec les personnes ne disposant pas de Silence et peut être utilisée comme application SMS par défaut.

Pour ces deux applications, il est recommandé d'activer le verrouillage de l'application et le chiffrement de ses données par une phrase de passe. Cela empêchera toute personne qui obtiendrait votre téléphone déchiffré d'accéder à vos communications sans ce code.

> Pour cela, aller dans Paramètres, Vie privée, Activer le verrouillage et entrer un code.

D'autres applications libres proposent la protection des communications par du chiffrement bout-en-bout, par exemple, Riot.im, Wire ainsi que le projet Briar, mais restent, pour le moment, plus marginales en nombre d'utilisateurs.

Le CECIL déconseille par ailleurs l'usage de Telegram qui malgré sa relative notoriété et une solution de chiffrement des échanges activable n'est pas libre aussi bien en ce qui concerne l'application que sur les méthodes de chiffrement. Son algorithme de chiffrement n'est donc pas auditable et sa sécurité est loin d'être prouvée. De plus, l'application ne propose pas le chiffrement par défaut des conversations, malgré la croyance, ni celui des conversations en groupe. Le CECIL déconseille également l'usage de WhatsApp qui s'appuie pourtant sur le protocole de chiffrement de Signal, mais qui est détenu par Facebook qui a tout fait pour exploiter les numéros de téléphone des personnes utilisant WhatsApp avec les données de Facebook et certaines métadonnées.

Des systèmes d'exploitation libres : Lineage OS

Android, le système d'exploitation de Google a été construit sur la base de logiciels libres et son noyau est donc libre et théoriquement librement réutilisable. Google a toutefois su parfaitement exploiter les avantages de « l'*open source* » (contributions volontaires bénévoles, reprises d'éléments de code existant…) tout en essayant de bloquer toutes les formes de concurrence par des partenariats agressifs avec les constructeurs imposant l'installation des « Google Mobile Services » (GMS) par défaut et en interdisant le recours à des dérivés ("*forks*") d'Android. Google contrôle également l'accès au « Google Play Store » qui s'est par ailleurs imposé comme un accès quasi-nécessaire à de nombreuses applications et a d'autres pratiques similaires. À l'exception des Iphone, le système d'exploitation Android monopolise désormais le marché.

Face à cette situation de nombreux projets ont vu le jour pour mettre en place un système d'exploitation pour ordiphone fiable et libéré de Google, mais la tâche est ardue et beaucoup ont été abandonnés face à ces contraintes. Il existe toutefois des projets qui tiennent bon et permettent dans certains cas de libérer son ordiphone de la mainmise de Google et des GMS. La solution la plus répandue et que le CECIL recommande est Lineage OS.

Fork du projet « Cyanogen » s'appuyant sur les éléments libres d'Android, Lineage constitue pour le moment l'alternative la plus simple pour « dégoogliser » un ordiphone sous Android.
Reste que le remplacement de son système d'exploitation sur ordiphone n'est pas aussi aisé que de remplacer Windows sur un ordinateur fixe. Il est nécessaire tout d'abord de pouvoir obtenir les droits administrateurs (dits *root*) sur son appareil, ce qui n'est pas toujours évident ainsi que de disposer d'un « portage » de Lineage spécifique à son appareil, les composants et interactions des différents modèles étant susceptibles de varier grandement.

Ainsi, si sur certains téléphones très achetés et bien documentés (cela peut constituer un éventuel critère de choix dans l'acquisition d'un appareil), le remplacement d'Android par Lineage peut s'avérer relativement aisé pour une personne suivant strictement les instructions et un peu débrouillarde, pour d'autres la tâche peut s'avérer complexe. Une telle opération est par ailleurs susceptible de compliquer une mise en œuvre de la garantie.

Pour qui souhaiterait sauter le pas, en plus de devoir se documenter sérieusement, il existe quelques personnes très motivées et prêtes à aider pour réaliser ce passage. Pour les rencontrer, de bons points d'entrée sont les forums spécialisés ainsi que les « fêtes d'installations » du monde du libre.

Des appareils plus éthiques à soutenir

Les ordinateurs de poche ne posent pas seulement des problèmes en termes de sécurité et de respect des libertés, les questions de réparabilité et de coûts écologiques, mais aussi de provenance des minéraux pour les fabriquer (problématique des « terres rares » provenant de zone de conflits et d'exploitation des mines où travaillent parfois des enfants), l'exploitation d'ouvrièr·es dans la fabrication, etc. posent d'importants enjeux de société.
Une alternative viable sur ces questions est portée par Fairphone. Cette entreprise Néerlandaise a été fondée en 2013 avec pour objectif de concevoir un ordiphone plus respectueux de l'environnement et d'améliorer les conditions productions, de travail et d'extraction :
* pas d'approvisionnement dans les zones de guerre ou permettant le travail des enfants,
* logique de commerce équitable,
* amélioration des conditions de travail,
* objectif de réparabilité maximale,
* recyclage des déchets électroniques.

Difficile d'être parfait en la matière et face aux contraintes économiques Fairphone a du par exemple arrêter la fourniture des pièces détachées pour le « Fairphone 1 » limitant de fait sa réparabilité et la durée de vie de cette première mouture. Le prix du Fairphone 2 désormais distribué reste élevé (> 500€). Fourni par défaut avec Android, il est par contre facile de le remplacer par « Fairphone Open » qui est un portage de Lineage pour le Fairphone.
Malgré quelques défauts, Fairphone a le mérite d'exister et de rechercher une certaine éthique sur des sujets facilement négligés face à des mobiles moins chers (au prix des conditions de travail à Shenzen et d'approvisionnement sanglant de certains matériaux) ou des approches marketing plus soignées. Les enjeux sont pourtant de taille en termes de droits humains et justifient de soutenir cette initiative.

On peut enfin signaler que bien que son usage se soit imposé socialement, la place et l'intérêt des ordiphones méritent d'être questionnés, la meilleure solution pour limiter ses problématiques restant encore de ne pas en acquérir.

Maxime Lehmann stagiaire au CECIL a participé à l'élaboration de cette fiche.

Pour aller plus loin

Des guides généraux sur la sécurisation des ordiphones et le paramétrage

- Gee, sur son blog Grisebouille.net, "Fairphone un téléphone pour libriste", qui détaille ses étapes pour "dégoogliser" au mieux son ordiphone et ses applications ;
- Sur le site de la Cnil.fr, "Maitriser les réglages vie privée de votre smartphone", 5 janv. 2015 et "Comment sécuriser au maximum l'accès à votre smartphone ?", 27 janv. 2017 ;
- Les guides de l'EFF, "Guides sur les outils" ;
- Anssi, ssi.gouv.fr, "recommandations de sécurité relatives aux ordiphones" ;
- Guide de l'association Nothing 2 Hide, "Protégez vos anonymats sur téléphone portable" ;
- A. Hern, TheGuardian.com, "Your battery status is being used to track you online" (en anglais) ;
- Freedom of the presse foundation, "Mobile security prevention tips" (en anglais).

Sur les applications libres et la sécurisation

En plus des applications citées, il est pertinent de se renseigner sur :
* AFWall +, qui permet sur un ordiphone "rooté" de bloquer l'accès à Internet d'application qui n'en ont pas besoin ;
* Haven, développée par le Guardian Project en collaboration avec E. Snowden qui permet d'utiliser les capteurs de l'ordiphone à des fins de sécurisation face à des atteintes extérieures illégitimes.

Sur la question du chiffrement sur ordiphone

- Voir les autres travaux du Guardian Project sur leur site Guardianproject.info ;
- M. Shelton, sur Medium.com, Signal for begginers", 18 nov. 2016 (en anglais) ;
- Sur la critique de Telegram, The Grugq sur Medium.com, "Operatinal Telegram", 18 nov. 2015 (en anglais) ;
- Il est possible de faire fonctionner PGP sur son ordiphone via K9-Mail en utilisant OpenKeychain, voir le tutoriel "Open Keychain Usage" sur le site k9mail.github.io ;
- Il est aussi possible d'utiliser un client XMPP et "Off The Record" sur ordiphone par exemple avec Xabber ou Conversations ;
- Il faut relever que le chiffrement des ordiphones fait l'objet de vifs débats publics et est très attaqué comme dans le cas de l'affaire "FBI vs Apple". En France, le fait de refuser de déchiffrer son appareil sur demande d'une autorité judiciaire peut potentiellement être sanctionné en tant que tel.

Sur les systèmes libres

- Le site Internet Lineageos.org ;
- On peut aussi découvrir différents projets essayant de porter un système d'exploitation libre pour ordiphone : UBPorts, Sailfish OS, Replicant, LuneOS, QubeOS Librem et le récent Eelo qui bénéficie d'un financement participatif réussi.

Enfin, pour questionner la place de l'ordiphone dans sa vie, Lapalice.fr, "Sans smartphone point de salut", le 21 fév. 2018.

Fiche 13 [publiée le 25 mai 2018]