Dois-je donner mon code de téléphone aux FDO ?

Cette page vise à tenter de répondre à cette question mais **la situation est encore mouvante** sur le sujet.

De quel code parle-t-on ?

On se pose souvent la question autour du code PIN du téléphone mais tout ce qui suit peut s'appliquer aux codes de téléphones, d'ordinateurs, de tablettes mais aussi de tout code relatif à des applications (gestionnaire de mot de passe, messagerie Signal, compte Mattermost...). L'article de loi sur lequel les FDO s'appuient pour demander le code explique qu'il s'agit de la "convention secrète de déchiffrement d'un moyen de cryptologie", cela peut donc s'appliquer à tous les appareils et applications.

Un FDO peut-il me demander mon code alors ?

La réponse est oui !

Cependant, pour ce faire, l'OPJ doit apporter la démonstration que le dispositif physique ou applicatif auquel iel essaie d'accéder est chiffré et qu'il n'y a pas d'autres moyens d'accéder aux données auxquelles iel veut accéder et que ces appareils ou applications sont soupçonnées d'avoir été utilisées pour préparer, faciliter ou commettre un crime ou un délit. La démonstration peut être par exemple la notice technique de Signal qui montre que tous les messages sont cryptés ou alors l'avis d'un·e technicien·ne expert·e qui affirme ne pas pouvoir accéder aux données d'un téléphone sans le code. Attention, peut être que dans un futur proche, on pourra nous rétorquer que quasi tous les smartphones sont cryptés donc le téléphone est sûrement crypté et ça pourrait suffir comme preuve.

Si l'OPJ n'apporte pas cette preuve, ce qui est quand même assez courant pour l'instant (octobre 2023), **on n'a pas à donner son code.**

Mais qu'est-ce qu'on risque à ne pas donner son code ?

C'est un délit passible de 3 ans de prison et 270 000 € d'amende.

Mais, c'est une infraction à mettre en balance avec d'autres points ultra importants :

- il peut y avoir des preuves vous incriminant dans votre téléphone, cela donnerait aux OPJ des éléments à charge sur ce qu'on vous reproche ;
- **vous mettez potentiellement en danger tous vos camarades et copaines.** L'OPJ pourrait potentiellement accéder à Signal, Mattermost, Protonmail et trouver des informations sur d'autres personnes, sur d'autres actions passées ou à venir, sur nos lieux de réunions...

La proposition du GST juridique serait donc de **ne jamais donner nos codes de téléphone**, sauf si on est sûr·es qu'il est propre. Nous avons tous·tes collectivement beaucoup plus à perdre à donner nos codes.

Mais comment on se protège de ça alors ??

> En ne venant pas en action avec nos téléphones. Ou alors avec des téléphones d'actions dédiés super propres.

Sur ce wiki, il existe plusieurs pages permettant de vous aider à sécuriser vos outils numériques : Hygiène numérique | Wiki XR (extinctionrebellion.fr) ou encore Sécuriser son téléphone | Wiki XR (extinctionrebellion.fr) et Sécuriser son ordinateur | Wiki XR (extinctionrebellion.fr)

Mais si je donne pas, la police peut craquer mon appareil électronique ??

La réponse est potentiellement oui !

Quasi tous les appareils sont craquable. Mais cela a un coût, qui peut être très élevé pour des appareils récents, cryptés et bien sécurisés. Les FDO n'utiliseront *a priori* ces techniques uniquement pour des délits très grave ou des crimes.

Textes juridiques

Article 434-15-2 du code pénal

Cour de Cassation - Assemblée plénière 7 novembre 2022

Quelques sources

Le sujet n'étant pas tranché, voici quelques éléments pour tenter d'y voir plus clair :

- Article de Paris Luttes Info
- Post Instagram d'Alexis Baudelin

Créé 2023-10-26 14:05:32 CEST par zak
Mis à jour 2023-11-05 17:15:01 CET par zak