



Surveillance policière : se protéger de son téléphone et de Whatsapp !

À la frontière franco-britannique comme ailleurs, de nombreux indices laissent penser que la police française surveille à distance le contenu des communications Whatsapp de nombreuses personnes, en particulier des gens qu'elle soupçonne de vouloir franchir la frontière clandestinement.

De nombreuses enquêtes sont en cours à la frontière franco-britannique pour arrêter les « passeurs ». La définition du mot « passeur » par les autorités est très controversée : il est illégal d'aider quelqu'un à traverser la frontière clandestinement, même gratuitement, et la police arrête beaucoup de gens pour ça. À cause de ça, certaines personnes sont envoyées en prison et parfois expulsées de France ensuite.

Lors d'une enquête de police en France, **il est simple pour la police de surveiller les conversations téléphoniques** juste en connaissant le numéro de téléphone qu'elle veut surveiller. Elle n'a pas besoin d'accéder physiquement au téléphone de quelqu'un. Le téléphone peut être surveillé pendant plusieurs mois par la police sans que la personne qui est surveillée ne s'en rende compte. Si la police vous surveille, elle peut donc écouter vos conversations téléphoniques et lire vos SMS.

Même si vous n'êtes pas surveillé.e, certaines informations sont quand même conservées pendant au moins 2 ans par votre opérateur et la police pourrait les consulter plus tard : la **géolocalisation de votre téléphone même si l'option GPS était désactivée**, avec quels numéros vous avez échangé des SMS et des appels, la durée des appels, ainsi que le détail des jours et des heures précises de chaque SMS, appel et géolocalisation. La géolocalisation de votre téléphone peut servir à la police pour vous trouver en temps réel afin de vous arrêter, ou en cas de procès pour prouver que vous étiez quelque part à un moment précis. L'historique de vos SMS et appels, même dans le cas où la police n'a pas accès au contenu, permet de savoir avec qui vous êtes en contact et quand.

La police a plein de manières de connaître votre numéro de téléphone :

- En demandant au vendeur de téléphone ou de crédit.
- Si elle vous arrête avec votre téléphone.
- Si elle trouve votre numéro de téléphone dans le répertoire téléphonique de quelqu'un d'autre après une arrestation ou une surveillance.
- En cherchant tous les téléphones qui étaient à un endroit précis à une heure précise. Par exemple, pour identifier les gens qui essaient de traverser la mer clandestinement : tous les téléphones détectés à 2h du matin sur une plage française proche de l'Angleterre.
- En installant un dispositif d'interception. Par exemple, un policier en civil cache une petite antenne dans son sac à dos et passe à côté de vous ; il pourra ensuite voir votre numéro si votre téléphone était allumé. Cela peut aussi marcher à plusieurs dizaines de mètres de distance avec un appareil plus gros, que les policiers peuvent cacher dans un véhicule.



Surveillance policière : se protéger de son téléphone et de Whatsapp !

À la frontière franco-britannique comme ailleurs, de nombreux indices laissent penser que la police française surveille à distance le contenu des communications Whatsapp de nombreuses personnes, en particulier des gens qu'elle soupçonne de vouloir franchir la frontière clandestinement.

De nombreuses enquêtes sont en cours à la frontière franco-britannique pour arrêter les « passeurs ». La définition du mot « passeur » par les autorités est très controversée : il est illégal d'aider quelqu'un à traverser la frontière clandestinement, même gratuitement, et la police arrête beaucoup de gens pour ça. À cause de ça, certaines personnes sont envoyées en prison et parfois expulsées de France ensuite.

Lors d'une enquête de police en France, **il est simple pour la police de surveiller les conversations téléphoniques** juste en connaissant le numéro de téléphone qu'elle veut surveiller. Elle n'a pas besoin d'accéder physiquement au téléphone de quelqu'un. Le téléphone peut être surveillé pendant plusieurs mois par la police sans que la personne qui est surveillée ne s'en rende compte. Si la police vous surveille, elle peut donc écouter vos conversations téléphoniques et lire vos SMS.

Même si vous n'êtes pas surveillé.e, certaines informations sont quand même conservées pendant au moins 2 ans par votre opérateur et la police pourrait les consulter plus tard : la **géolocalisation de votre téléphone même si l'option GPS était désactivée**, avec quels numéros vous avez échangé des SMS et des appels, la durée des appels, ainsi que le détail des jours et des heures précises de chaque SMS, appel et géolocalisation. La géolocalisation de votre téléphone peut servir à la police pour vous trouver en temps réel afin de vous arrêter, ou en cas de procès pour prouver que vous étiez quelque part à un moment précis. L'historique de vos SMS et appels, même dans le cas où la police n'a pas accès au contenu, permet de savoir avec qui vous êtes en contact et quand.

La police a plein de manières de connaître votre numéro de téléphone :

- En demandant au vendeur de téléphone ou de crédit.
- Si elle vous arrête avec votre téléphone.
- Si elle trouve votre numéro de téléphone dans le répertoire téléphonique de quelqu'un d'autre après une arrestation ou une surveillance.
- En cherchant tous les téléphones qui étaient à un endroit précis à une heure précise. Par exemple, pour identifier les gens qui essaient de traverser la mer clandestinement : tous les téléphones détectés à 2h du matin sur une plage française proche de l'Angleterre.
- En installant un dispositif d'interception. Par exemple, un policier en civil cache une petite antenne dans son sac à dos et passe à côté de vous ; il pourra ensuite voir votre numéro si votre téléphone était allumé. Cela peut aussi marcher à plusieurs dizaines de mètres de distance avec un appareil plus gros, que les policiers peuvent cacher dans un véhicule.

Même s'ils sont pratiques, **nos téléphones sont de véritables espions pour la police !**

Face à cela, **pour empêcher la géolocalisation de son téléphone, la seule solution est de le mettre en mode avion**, voire dans l'idéal de l'éteindre et d'enlever sa batterie. Dès que le téléphone est allumé, même si le GPS est désactivé, il borne sur le réseau qui enregistre sa localisation. Pour compliquer la surveillance de vos messages et appels, le mieux est d'utiliser des messageries sur internet avec un chiffrement de bout-en-bout, afin que la communication ne soit visible que par vous et vos interlocuteurs.

Whatsapp est une application de messagerie en ligne qui appartient à l'entreprise américaine Meta, qui possède aussi Facebook, Messenger et Instagram. L'entreprise prétend utiliser le chiffrement de bout-en-bout pour sa messagerie, et donc que personne ne peut intercepter un appel ou un message à part la personne qui l'envoie et la personne qui le reçoit. Mais le protocole de sécurité Whatsapp est tenu secret puisque l'entreprise refuse de le révéler. Il n'est donc pas possible de savoir s'il existe des failles dans la sécurité de Whatsapp que la police peut utiliser pour surveiller les utilisateurs. **De nombreux indices laissent penser que dans certaines enquêtes, les policiers arrivent à écouter les messages et appels Whatsapp.** Sur son site internet, Whatsapp indique collaborer avec les autorités pour la surveillance de ses utilisateurs.

Une alternative pour se protéger est l'application Signal. Son utilisation est facile et ressemble beaucoup à celle de Whatsapp. Mais le protocole de sécurité de Signal est open-source : il est accessible à tout le monde et chacun-e peut vérifier qu'il n'y a pas de faille qui permette à la police ou à d'autres personnes malveillantes d'intercepter les communications. Des milliers d'informaticien-nes dans le monde surveillent et améliorent chaque jour la sécurité de Signal, en toute transparence. Cela ne veut pas dire que Signal est infaillible, mais il y a plus de raisons de lui faire confiance que Whatsapp. Par ailleurs, Signal est une entreprise à but non-lucratif, alors que Whatsapp gagne de l'argent en collectant et revendant les données de ses utilisateurs, c'est une raison de plus pour préférer Signal à Whatsapp !

Pour installer Signal, c'est simple, il suffit de télécharger « Signal Private Messenger » sur votre smartphone :

- Sur les appareils Android, dans l'application GooglePlay.
- Sur iPhone ou iPad, dans l'application AppStore.



Une fois l'application installée, vous aurez juste à créer un compte avec un code validation par SMS. Conseil de sécurité : quand vous créez votre profil, mettez un pseudo plutôt que votre vrai nom. Une fois votre compte créé, vous pourrez communiquer avec tous vos contacts qui utilisent aussi Signal : messages écrits, messages vocaux, photos, vidéos, appels, conversation de groupes... Cela marche uniquement avec les personnes qui ont aussi installé Signal sur leur téléphone, donc invitez vos amis et votre famille à l'installer aussi pour pouvoir communiquer ensemble de manière plus sécurisée.

Attention ! Si un jour la police vous arrête avec votre téléphone, il est possible qu'elle l'ouvre et lise vos messages Signal, même si vous avez mis un code. Si elle arrête une personne avec qui vous êtes en contact, elle peut de la même manière lire les messages que vous lui avez envoyé. Pensez donc à effacer régulièrement vos messages. Dans les paramètres de Signal, il est possible de mettre l'option « messages éphémères » pour régler l'effacement automatique des messages après un certain délai.

Luttons contre la surveillance ! La vie privée est un droit humain !

Même s'ils sont pratiques, **nos téléphones sont de véritables espions pour la police !**

Face à cela, **pour empêcher la géolocalisation de son téléphone, la seule solution est de le mettre en mode avion**, voire dans l'idéal de l'éteindre et d'enlever sa batterie. Dès que le téléphone est allumé, même si le GPS est désactivé, il borne sur le réseau qui enregistre sa localisation. Pour compliquer la surveillance de vos messages et appels, le mieux est d'utiliser des messageries sur internet avec un chiffrement de bout-en-bout, afin que la communication ne soit visible que par vous et vos interlocuteurs.

Whatsapp est une application de messagerie en ligne qui appartient à l'entreprise américaine Meta, qui possède aussi Facebook, Messenger et Instagram. L'entreprise prétend utiliser le chiffrement de bout-en-bout pour sa messagerie, et donc que personne ne peut intercepter un appel ou un message à part la personne qui l'envoie et la personne qui le reçoit. Mais le protocole de sécurité Whatsapp est tenu secret puisque l'entreprise refuse de le révéler. Il n'est donc pas possible de savoir s'il existe des failles dans la sécurité de Whatsapp que la police peut utiliser pour surveiller les utilisateurs. **De nombreux indices laissent penser que dans certaines enquêtes, les policiers arrivent à écouter les messages et appels Whatsapp.** Sur son site internet, Whatsapp indique collaborer avec les autorités pour la surveillance de ses utilisateurs.

Une alternative pour se protéger est l'application Signal. Son utilisation est facile et ressemble beaucoup à celle de Whatsapp. Mais le protocole de sécurité de Signal est open-source : il est accessible à tout le monde et chacun-e peut vérifier qu'il n'y a pas de faille qui permette à la police ou à d'autres personnes malveillantes d'intercepter les communications. Des milliers d'informaticien-nes dans le monde surveillent et améliorent chaque jour la sécurité de Signal, en toute transparence. Cela ne veut pas dire que Signal est infaillible, mais il y a plus de raisons de lui faire confiance que Whatsapp. Par ailleurs, Signal est une entreprise à but non-lucratif, alors que Whatsapp gagne de l'argent en collectant et revendant les données de ses utilisateurs, c'est une raison de plus pour préférer Signal à Whatsapp !

Pour installer Signal, c'est simple, il suffit de télécharger « Signal Private Messenger » sur votre smartphone :

- Sur les appareils Android, dans l'application GooglePlay.
- Sur iPhone ou iPad, dans l'application AppStore.



Une fois l'application installée, vous aurez juste à créer un compte avec un code validation par SMS. Conseil de sécurité : quand vous créez votre profil, mettez un pseudo plutôt que votre vrai nom. Une fois votre compte créé, vous pourrez communiquer avec tous vos contacts qui utilisent aussi Signal : messages écrits, messages vocaux, photos, vidéos, appels, conversation de groupes... Cela marche uniquement avec les personnes qui ont aussi installé Signal sur leur téléphone, donc invitez vos amis et votre famille à l'installer aussi pour pouvoir communiquer ensemble de manière plus sécurisée.

Attention ! Si un jour la police vous arrête avec votre téléphone, il est possible qu'elle l'ouvre et lise vos messages Signal, même si vous avez mis un code. Si elle arrête une personne avec qui vous êtes en contact, elle peut de la même manière lire les messages que vous lui avez envoyé. Pensez donc à effacer régulièrement vos messages. Dans les paramètres de Signal, il est possible de mettre l'option « messages éphémères » pour régler l'effacement automatique des messages après un certain délai.

Luttons contre la surveillance ! La vie privée est un droit humain !