Mathieu Cunche : “Aucune application de messagerie n’est parfaite”

Emile Marzolf

Faut-il, comme l’a fait la Première ministre, **interdire les applications de messagerie instantanée “grand public” aux ministres et conseillers ministériels, et plus largement aux agents publics ?**
Tout est une question de sensibilité des informations échangées et des personnes avec lesquelles elles sont échangées. Les 2 éléments sont importants, aussi bien le contenu des messages que l’identité des interlocuteurs, car il existe de nombreuses situations dans lesquelles les simples métadonnées *[informations techniques relatives à l’échange lui-même, comme l’heure d’envoi, ndlr]* peuvent révéler de l’information à un observateur extérieur, et notamment à l’entreprise qui fournit le service de messagerie. Le chiffrement de bout en bout offre une première garantie pour la protection du contenu des messages, mais uniquement sur le papier, car il est très difficile d’auditer les applications et surtout les serveurs sur lesquels elles sont déployées. Il est possible de le faire en partie avec Signal, qui est en *open source,* mais là encore, on ne peut pas vérifier que le code publié est bien celui qui tourne sur les machines.

Y a-t-il une application qui sort du lot ?
Je ne saurais pas dire laquelle est la plus sécurisée. Mais l’ouverture du code source est en tout cas une première étape indispensable pour le vérifier. Signal est très utilisée dans le monde, et son code a donc été largement audité. Ce n’est pas le cas de WhatsApp, ni d’Olvid. Cette dernière a tout de même soumis son code à des audits externes et publié sa documentation. Et quand bien même le chiffrement de bout en bout serait efficace pour cacher le contenu des messages, la question des métadonnées demeure une menace. Prenons l’exemple de la préparation d’un déplacement impromptu et secret d’Emmanuel Macron, en France ou dans un pays étranger, il pourrait être “trahi” par le recoupement des métadonnées des différentes communications. Des études montrent qu’il est possible de deviner quel site Web consulte un internaute, quand bien même il navigue sur un canal chiffré, ou bien encore les objets connectés qu’il possède rien qu’en regardant la destination des communications. Et il ne faut pas oublier non plus qu’il est possible d’identifier une personne à partir de ses seuls contacts. Il faut aussi rappeler que le simple fait d’utiliser des applications non maîtrisées sur son téléphone constitue déjà une menace. Certaines applications vulnérables peuvent servir de vecteurs d’attaque. L’application de messagerie est elle aussi plus ou moins “curieuse” et peut collecter différentes données ici ou là sur le téléphone.

Pour évaluer une application, il faut regarder deux choses : d'abord, est-ce que le code et les spécifications techniques sont ouverts et donc auditables, et ensuite, qui est derrière cette application et quel est son modèle économique.

Est-ce une idée pertinente de bannir WhatsApp, qui a fait l'objet d'une note d'alerte de l'Agence nationale de la sécurité des systèmes d'information dès 2021 **?**
Je suis très surpris d'apprendre que nos ministres utilisent WhatsApp. On connaît bien le *business model* de Meta, qui repose sur la commercialisation des données des utilisateurs. Et on peut s'interroger sur ce qu'ils font avec WhatsApp, quand on voit la liste des permissions demandées pour activer l'application : accès à la caméra, à la connexion Bluetooth, au répertoire de contacts, ou même à la géolocalisation. Qu'advient-il de ces données ? Peut-être rien, mais on ne peut pas le savoir car l'application est complètement opaque. Sans oublier le risque qu'elles soient transmises aux autorités américaines, révélé par l'affaire Snowden.

Qu'en est-il des autres applications, et en particulier d'Olvid, promue par la Première ministre, Élisabeth Borne, dans sa circulaire ?
Toutes ces applications revendiquent la confidentialité des communications grâce au chiffrement de bout en bout, et revendiquent un niveau de sécurité semblable, avec des protocoles finalement similaires. Tout dépend donc de leur mise en œuvre, qui reste assez opaque. Olvid est, elle, un peu différente dans son architecture, mais surtout, elle n'utilise pas les numéros de téléphone comme identifiants d'utilisateur, ce qui peut être un avantage en matière de protection de la vie privée. En revanche, cela complique la découverte des contacts et donc la prise en main de l'application par de nouveaux utilisateurs. Or ce genre d'applications fonctionne comme un réseau social : elles n'ont aucun intérêt si vous êtes seuls à l'utiliser. Aucune application n'est donc parfaite, mais pour les évaluer, il faut regarder deux choses : d'abord, est-ce que le code et les spécifications techniques sont ouverts et donc auditables, et ensuite, qui est derrière cette application et quel est son modèle économique. WhatsApp est gratuit, Signal s'appuie sur une fondation à but non lucratif et Olvid propose un modèle gratuit avec une offre payante pour les entreprises et les institutions, et a le mérite d'être française, mais je ne serais pas capable de vous dire qu'Olvid est préférable à Signal.

Propos recueillis par Émile Marzolf