Payer Apple et Google pour le déchiffrement ?

Les autorités américaines sont très critiques envers les solutions de chiffrement mises en place par des acteurs comme Google et Apple sur leurs terminaux. FBI, NSA, CIA veulent avoir un accès aux informations chiffrées au nom de la sécurité nationale pour prévenir des attaques ou des menaces. Les acteurs IT ont pour l'instant refusé en assurant qu'ils doivent garantir la sécurité des données de leurs clients. Plusieurs scénarios ont été proposés pour réconcilier les intérêts de chacun, mise d'une porte d'entrée à plusieurs serrures, création d'un site miroir sur décision d'un juge. En vain.

Le professeur Darren Hayes, directeur de la chaire cybersécurité à la Pace University propose une autre alternative : la rétribution financière. Pour lui, « *s'il existait une incitation financière à Google et Apple pour aider les autorités judiciaires, alors ils seraient amenés à changer leur technologie de chiffrement et faciliter le travail des enquêteurs mandatés* ».

Réviser la loi sur les écoutes téléphoniques

Pour sa démonstration, il compare cette demande avec l'obligation des opérateurs télécommunications en matière d'écoutes téléphoniques sur instruction judiciaire. La loi CALEA (Communications Assistance for Law Enforcement Act) de 1994 prévoit une compensation financière pour cette aide. Selon l'universitaire, cette rétribution est « *assez bonne* ». Il n'oublie pas que les deux sociétés Google et Apple ont comme objectif de réaliser des profits. Elles pourraient rapidement faire leur calcul pour apporter cette aide contre rétribution. Pour cela, le professeur propose de réviser la loi CALEA pour intégrer le chiffrement des données.

Apple et Google n'ont pas souhaité commenter cette proposition, mais le Information Technology Industry Council, qui comprend les deux sociétés, est opposé à toutes tentatives pour casser ou contourner le chiffrement. Tim Cook l'a encore rappelé dans une interview à CBS.

Le débat n'est donc pas prêt de s'arrêter sur le sujet. Surtout avec les récentes découvertes établissant des liens directs entre les messageries chiffrées Telegram et WhatsApp et la préparation des attentats de Paris.

A lire aussi :

Le procureur de Paris prend position contre le chiffrement des smartphones

WiFi interdit, Tor bloqué, backdoors : les services de police en roue libre

Après les attentats : faut-il mieux encadrer le chiffrement ?

Crédit photo : Maksim Kabakou / Shutterstock