Chiffrement : un projet de loi aux Etats-Unis pour forcer l'industrie à collaborer

Fermer la porte à des différends du type de celui qui a opposé Apple au FBI dans l'affaire du déblocage de l'iPhone d'un des auteurs de la tuerie de San Bernardino. Deux sénateurs américains, un Républicain et un Démocrate, viennent de déposer un projet de loi qui obligerait les entreprises à aider les forces de l'ordre dans leur tentative de déchiffrement de données ou de déblocage de terminaux.

Dévoilée vendredi dernier par les **sénateurs Richard Burr et Dianne Feinstein**, la proposition permettrait aux juges d'enjoindre les entreprises de la tech à apporter leur assistance aux efforts du FBI et autres forces de sécurité. « *Toute personne recevant une injonction de la justice pour fournir des informations ou des données doit fournir, dans un délai raisonnable, avec une bonne réactivité, ces données ou informations de façon intelligible ou une assistance technique appropriée* », peut-on lire dans la proposition Burr – Feinstein. Pour les forces de l'ordre, ce texte leur permettrait de trouver **un terrain juridique solide** pour leurs demandes d'assistance à l'attention du secteur privé (pour l'instant, comme dans le cas d'Apple, les juges s'appuient sur une disposition très ancienne).

« *Paradoxe intenable* »

Évidemment, ce projet de loi a toutes les chances de se heurter à une opposition farouche de la Silicon Valley, qui avait pris fait et cause pour Apple dans son combat contre le FBI. Dans un communiqué, l'Information Technology and Innovation Foundation (Itif), un think tank de Washington défendant les intérêts de l'industrie, estime que cette loi placera les entreprises américaines devant un « *paradoxe intenable* ». Pour le groupe de pression, « *la politique du gouvernement américain devrait être d'améliorer la cybersécurité, pas de l'affaiblir* ».

Dans les faits, si elle est votée, cette législation placerait dans une situation inconfortable les entreprises fournissant du chiffrement de bout en bout, dont les clefs sont détenues par les utilisateurs eux-mêmes. « *Par exemple, la populaire application de messagerie WhatsApp, qui fournit du chiffrement de bout en bout sur sa plate-forme, ne serait pas en masure d'être en conformité avec la loi, sauf à modifier son système* », relève le vice-président de l'Itif, Daniel Castro. Pour respecter la législation, la société n'aurait d'autre choix que d'inclure une backdoor permettant, sur requête d'un juge, de décoder les échanges d'un utilisateur.

Dans l'affaire portant sur le déblocage de l'iPhone d'un des tueurs de San Bernardino, le FBI demandait à Apple de développer une mise à jour de son OS, que la firme est la seule à pouvoir signer pour qu'elle soit acceptée par ses terminaux, permettant de contourner les sécurités d'iOS (notamment le nombre limité d'essais pour entrer le code PIN de l'utilisateur). Cupertino avait refusé, mais les enquêteurs américains sont tout de même parvenus à débloquer le smartphone, probablement grâce à une technique mise au point par la start-up israélienne Cellebrite**. Une technique restée confidentielle à ce jour.**

En France aussi ?

En France, dans le cadre de la discussion sur le projet de loi de réforme pénale contre le crime organisé, un amendement proposé par un groupe de députés Les Républicains, et voté en première lecture, prévoit : « *le fait, pour un organisme privé, de refuser de communiquer à l'autorité judiciaire requérante enquêtant sur des crimes ou délits terroristes (…) des données protégées par un moyen de cryptologie dont il est le constructeur, est puni de cinq ans d'emprisonnement et 350 000 euros d'amende* ». Un amendement du député LR Eric Ciotti, rejeté de justesse par l'Assemblée, entendait même aller jusqu'à l'interdiction temporaire de commercialisation pour les produits et services incriminés.

A lire aussi :

Sécurité de l'iPhone : pourquoi Apple s'est tiré une balle dans le pied

Crédit photo : Orhan Cam / shutterstock