

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes



Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18^e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.



« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (...) toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage », a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.

« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs « aveugles » dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.

L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « cassé » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.

Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les « téléphones cryptés ». « Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner », expliquait au Monde le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : « Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. » C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, « huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé », a détaillé M. Molins.

Concernant le cryptage, « il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données », assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par Le Monde.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, « cette possibilité semble ignorée par de nombreux services ». Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, « dans le cadre d'une urgence vitale », de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.

Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. « Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal... Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger », conclut le SCITT.



Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon