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

Même si les officiels français et américains se sont refusé à confirmer que les attentats de Paris ont été préparés via des moyens de chiffrement, la polémique a ressurgi sur la disponibilité de technologies permettant de garder les échanges électroniques hors de portée des services de sécurité. Dans une interview donnée ce matin à France Info, **Bernard Cazeneuve**, le ministre de l'Intérieur, confirme ainsi la volonté de la France d'investir dans des moyens électroniques pour lutter efficacement contre « *des acteurs terroristes qui dissimulent la commission de leurs actes grâce à des moyens cryptés* ».

Si Paris se montre pour l'instant peu disert sur la préparation des attentats qui ont visé Paris le 13 novembre, Washington a relevé que l'Etat islamique utilisait, depuis environ 18 mois, des technologies de chiffrement qui défiaient les moyens de la NSA. On pense ici à des applications comme Signal, Wickr et surtout **Telegram**, qui chiffre les messages des téléphones mobiles. L'Etat islamique s'est servi de cette application pour revendiquer la destruction du vol russe au-dessus du Sinaï – tuant ses 224 passagers – et les récents attentats de Paris.

Telegram : plus discret qu'un réseau social

Créé par Pavel Durov, fondateur du réseau social russe Vkontakte, Telegram, un service basé à Berlin, permet de créer des canaux de communication pouvant chacun réunir jusqu'à 200 utilisateurs. Dans un environnement chiffré, anonymisé et non modéré. Seuls les administrateurs ont connaissance des identités des utilisateurs. Selon une étude récente du Middle East Media Research Institute, tant l'Etat Islamique que Al-Qaïda dans la Péninsule Arabique se servent de ce canal pour diffuser leurs messages en plusieurs langues, y compris des tutoriels sur la préparation d'armes ou des appels à lancer des attentats.

Les soupçons des enquêteurs quant à l'utilisation de moyens de chiffrement ont relancé, outre Atlantique, le débat sur le contrôle de ces moyens par les Etats. Il y a quelques semaines, le Président Obama avait pourtant tranché, estimant, sur la base d'un rapport d'experts, que contraindre les fournisseurs de technologies à fournir les clefs au gouvernement ou à intégrer des backdoors serait sans effet. Rappelons que, suite aux révélations d'Edward Snowden, les entreprises de la Silicon Valley ont durci les fonctions de sécurité offertes à leurs utilisateurs. Apple a ainsi généralisé le chiffrement sur ses terminaux et déporté les clefs sur les machines elles-mêmes. Les éventuelles demandes d'assistance des services de renseignement auprès d'Apple sont donc, par construction, devenues inopérantes, Cupertino n'étant plus en possession des clefs.

Ce week-end, lors d'une émission de télévision sur CBS, le directeur adjoint de la CIA, Michael Morell, a estimé : « *Je pense qu'on va découvrir que ces individus (les terroristes de Paris, NDLR) communiquent avec des applications commerciales de chiffrement, qui sont très difficiles, voire impossibles à casser pour les gouvernements* ». D'autres officiels américains ont tenu des propos similaires, comme le chef de la police de New York, Bill Bratton qui a affirmé que ses services butent de plus en plus sur les fonctions de chiffrement offertes sur les smartphones par Apple ou Google (via Android).

Faute de pouvoir déchiffrer les communications, les services de sécurité doivent se contenter d'analyser les métadonnées des échanges électroniques.

Préparer un attentat sur… PlayStation ?

En août dernier, le procureur de la République de Paris, François Molins, co-signait une tribune dans le New York Times plaidant pour un affaiblissement du chiffrement. Et dénonçant le renforcement de la sécurité mis en œuvre par Apple et Google, changement qui ne serait pas passé inaperçu des malfaiteurs. Selon François Molins, ces derniers auraient aujourd'hui intégrés que les réquisitions de la justice portant sur les données de leurs smartphones resteront lettres mortes.

En l'état actuel de l'enquête, rien ne permet de dire quels moyens de communications ont utilisés les terroristes, dont la base arrière semble se situer à Bruxelles, pour échanger avec leurs commanditaires, en Syrie. Dans un entretien avec Politico trois jours avant les attentats, le ministre belge de l'Intérieur, Jan Jambon, soulignait l'usage par les fondamentalistes des communications sur… PlayStation 4. Des échanges qui se déroulent à l'intérieur de certaines parties et qui seraient très difficiles à repérer et intercepter, selon le ministre.

Dans un article de Buzzfeed News, un officier du renseignement américain, qui s'exprime de façon anonyme, détaille une autre des techniques utilisées par les terroristes : le découpage de l'information. « *Aujourd'hui, les agences de renseignement ont les capacités pour intercepter des messages chiffrés spécifiques et les décoder, si elles en ont le temps et les motivations. Mais, si en faisant cela, elle décrypte un message qui contient uniquement le mot 'demain' ou simplement 'la météo est bonne', en quoi cela nous aide-t-il ? Nous serons avertis que quelque chose risque d'arriver, mais nous ne saurons ni où, ni quand.* »

Signalons que le renseignement U.S. a averti la France il y a quelques semaines d'une possible attaque de l'État islamique. François Hollande avait alors décidé, début octobre, de mener une première série de frappes aériennes ciblées sur Raqqa, capitale de l'organisation terroriste.

A lire aussi :

Attentats terroristes à Paris : le chiffrement fait débat

Chiffrement : la NSA plaide pour un cadre légal d'accès aux communications

Crédit Photo : Isak55-Shutterstock