Apple prend la tête du combat contre les backdoors dans le chiffrement

L'arrivée d'un projet de loi britannique, raffermissant les prérogatives des services de sécurité, illustre bien la position inconfortable dans laquelle se trouvent les grands noms de la technologie, qui ont tous renforcé les outils de chiffrement mis à disposition de leurs clients après les révélations d'Edward Snowden sur la NSA américaine. La proposition de loi en question prévoit que les sociétés privées apportent leur concours aux autorités pour déchiffrer les données de leurs clients.

Apple, mais aussi Microsoft ou Yahoo, tentent de s'opposer à ce texte via une série d'arguments transmis à une commission en charge de l'examen de la future loi. Pour les firmes américaines, une telle législation ouvrirait la boîte de Pandore, d'autres pays étant susceptibles de rejoindre Londres en votant des mesures comparables, **y compris des régimes répressifs** qui pourraient arguer du fait que même les démocraties s'engagent dans cette voie. Apple et consorts expliquent par ailleurs que les mesures britanniques violeraient les législations d'autres pays.

« Une backdoor aussi pour les méchants »

Dimanche, Tim Cook a pris la **défense du chiffrement fort** lors de la célèbre émission de télévision 60 Minutes, diffusée par CBS. « *La réalité, c'est que si vous intégrez une backdoor dans vos outils, cette backdoor existe pour tous – pour les bons mais aussi pour les méchants* », a lancé le patron d'Apple. Un message qu'on retrouve dans l'argumentaire envoyé au gouvernement du Royaume-Uni : « *les meilleurs esprits au monde ne peuvent réécrire les lois mathématiques. Tout processus affaiblissant les modèles mathématiques qui protègent les données des utilisateurs, va par extension, affaiblir la protection* », écrit Apple, selon une copie du document obtenu par le Washington Post. Le projet de loi prévoit que Cupertino soit dans l'obligation de fournir un moyen d'écouter les conversations iChat et FaceTime sur iPhone.

De son côté, Yahoo anticipe des **conflits entre cette future législation et des lois d'autres pays**, estimant que le projet de loi de Londres revient « *à affirmer largement et de façon unilatérale la juridiction britannique outre-mer* ». Ce qui placerait les entreprises de la tech devant des choix cornéliens, quand l'administration britannique réclamera l'accès à des données stockées hors du pays. « *La législation doit éviter des conflits avec les lois d'autres pays et contribuer à un système où des gouvernements partageant le même esprit travaillent ensemble, et non dans un esprit de compétition, à la sécurité des personnes* », écrit de son côté Microsoft.

Un Projet Manhattan pour le chiffrement ?

La mobilisation de l'industrie américaine s'explique également par le débat actuel sur le chiffrement aux Etats-Unis, dans le cadre de la campagne présidentielle. Deux fois au cours des dernières semaines, **Hillary Clinton**, la candidate démocrate la mieux placée, a poussé la Silicon Valley à sortir de l'impasse où elle se trouve dans son dialogue actuel avec les services de sécurité

américains sur les communications chiffrés. Dimanche, elle a même appelé au lancement de l'équivalent d'un « Projet Manhattan » (nom de code du programme de développement de la bombe atomique américaine durant la Seconde guerre mondiale), réunissant le gouvernement et les communautés techniques, pour permettre aux industriels de se plier aux réquisitions judiciaires sans pour autant introduire de backdoor dans les technologies de chiffrement. Passons sur la cohérence technique d'un tel argumentaire…

De leur côté, les candidats républicains réclament que l'industrie high tech accorde aux services de renseignement et de police les accès aux données des smartphones et autres applications pratiquant le chiffrement de bout en bout. Le futur président des États-Unis a donc de bonnes chances d'adopter une position plus ferme vis-à-vis de l'industrie que celle de Barack Obama, même si l'actuel président de la première économie dans le monde a annoncé vendredi dernier sa volonté « *d'engager un dialogue avec la Silicon Valley* » pour mieux débusquer les activités terroristes. La Maison Blanche pourrait adopter une nouvelle position sur le chiffrement autour de la nouvelle année, explique la presse américaine.

En France aussi

C'est notamment **le FBI, via son directeur James Comey,** qui mène la charge contre le chiffrement fort. La semaine dernière encore, il a assuré, lors d'une conférence sur le terrorisme à New York, que « *l'utilisation du chiffrement est au cœur des techniques terroristes* ». Le FBI explique notamment n'être pas parvenu à décoder 109 messages échangés entre un terroriste et un correspondant en Syrie, connu pour être affilié à Daech, avant l'attentat de Garland, au Texas, en mai dernier.

En France également, après les attentats du 13 novembre, la tendance est au renforcement des dispositions permettant de généraliser les écoutes. En prenant des mesures complémentaires de celles déjà votés dans le cadre de la loi sur le renseignement. A la mi-novembre, **Bernard Cazeneuve**, le ministre de l'Intérieur, confirmait 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* ». Il y a quelques jours, CNN assurait, citant des sources officielles proches de l'enquête, que Telegram et WhatsApp, deux messageries proposant un chiffrement de bout en bout, avaient été employés dans le cadre de la préparation des attentats de Paris. Information qui n'a, pour l'instant, pas été confirmée officiellement par les autorités françaises.

Apple : des arguments inaudibles ?

Des deux côtés de l'Atlantique, les services de sécurité ciblent les technologies de chiffrement de bout en bout, dont les clefs restent entre les mains des utilisateurs. Souvent déployées après les révélations d'Edward Snowden, ces solutions ne permettent pas à l'industriel d'accéder au contenu des communications. Il se trouve donc dans l'**incapacité de se soumettre** aux requêtes officielles des services de renseignement ou des forces de l'ordre. Pour autoriser un accès aux données, Apple et Samsung seraient, par exemple, forcés de modifier l'OS de leurs smartphones. Depuis iOS 8 et Android 5.0 (Lollipop), les clefs de chiffrement sont en effet embarquées directement sur les terminaux, donnant aux utilisateurs un contrôle total sur leurs outils.

L’industrie de la high tech tente de faire valoir que créer une porte d’entrée pour les requêtes des services aboutirait à rendre vulnérable le système tout entier. Une vulnérabilité que ne manquerait pas d’exploiter des pays comme la Chine, la Russie ou la Corée du Nord. Dans son interview sur CBS, Tim Cook a tenté de faire valoir qu’opposer respect de la vie privée et sécurité « *relevait d’une vision simpliste* ». Pas sûr toutefois que le climat politique actuel rende cet argument suffisamment audible…

A lire aussi :

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

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

Le procureur de Paris prend position contre le chiffrement des smartphones