Le Monde.fr

SCQ
Les acteurs du Web vent debout contre un accès facilité à leurs données chiffrées

697 mots
26 novembre 2015
Le Monde Éco et entreprise
LEMECO
8
Français

Après les attentats du 13 novembre, plusieurs gouvernements ont remis le sujet sur la table

Faut-il ou non permettre aux forces de l'ordre et aux autorités judiciaires d'avoir accès à toutes les communications sur Internet ? Au lendemain des attentats du 13 novembre, le débat a repris de la vigueur aux Etats-Unis et au Royaume-Uni. Depuis l'affaire Snowden, qui a révélé les pratiques de surveillance de masse de la NSA, l'agence nationale de sécurité américaine, les géants du Web ont généralisé le chiffrement, c'est-à-dire le cryptage, à l'ensemble de leurs services.

Hors réquisitions judiciaires et sans l'aval des opérateurs du Net, impossible pour la police ou les services de renseignement de lire et d'écouter les conversations sur les messageries Gmail, Twitter, Facebook, WhatsApp ou Skype. Il y a dix-huit mois, Apple et Google ont franchi une étape supplémentaire en introduisant par défaut le chiffrement des données stockées dans les smartphones. " Historiquement, un logiciel comme FinFisher, vendu par la société Gamma, permettait à la police de lire très facilement ce qu'il y avait dans un mobile. Aujourd'hui, c'est devenu plus compliqué ", dit Gérome Billois, expert chez Solucom.

Même s'il n'apparaît pas que les terroristes aient utilisé des smartphones cryptés pour organiser les attaques, la Maison Blanche et le Congrès américain sont repartis à la charge contre les géants du Web, en demandant à leurs dirigeants de " sortir de cette impasse ", a révélé le Wall Street Journal. Les autorités rêvent que les grands acteurs de la tech leur donnent accès à leurs services, par une " porte dérobée ". Pour ces derniers, cela consisterait à introduire une faille dans leurs programmes.

" Sécurité affaiblie " Les géants du Net, dont le modèle économique repose sur la confiance accordée par leurs utilisateurs, sont vent debout contre ce type de mesure. " Affaiblir le chiffrement revient à affaiblir notre sécurité à tous - sur Internet - . Le chiffrement protège des milliards d'internautes contre d'innombrables menaces et contre les régimes gouvernementaux répressifs ", a lancé au site Politico Michael Beckerman, le président de l'Internet Association, qui représente les grands acteurs du Web. Avant lui, l'Information Technology Council, qui rassemble tous les grands groupes de technologies, assurait que ces portes dérobées pouvaient ensuite " être utilisées par les mauvaises personnes ".

" Les grands acteurs du Web s'inquiètent de l'utilisation qui serait faite de ces failles. Angela Merkel n'a pas été espionnée - par la NSA - à cause du terrorisme ", rappelle Nicolas **Arpagian**, directeur scientifique de l'Institut national des hautes études de la sécurité et de la justice.

Le débat dépasse l'Amérique. Au Royaume-Uni, le premier ministre, David Cameron, projette de faire voter une loi qui rendrait ces portes dérobées obligatoires. Une perspective contre laquelle Tim Cook, le patron d'Apple, s'est personnellement insurgé. En France, le ministre de l'intérieur, Bernard Cazeneuve, a indiqué le 17 novembre sur France Info qu'il souhaitait que les forces de l'ordre puissent être " efficaces " face " à des terroristes qui dissimulent leurs actes en utilisant des moyens cryptés sur Internet ". " Les signaux sur une future régulation se multiplient ", s'inquiète Tristan Nitot, ancien président de Mozilla Europe, chef de produit de Cozy Cloud, qui propose un système de protection des données personnelles

Cette figure du Net rappelle les risques qui menacent les internautes. " Sans le chiffrement, les sites Web ne sont pas protégés contre le “phishing” - qui permet à des pirates de dérober des données personnelles - ", commente Tristan Nitot.Face à ces fléaux, le chiffrement se développe à toute allure. Trois professionnels de la technologie, Mozilla, Cisco et Akamai, financent par exemple Let's Encrypt, une association qui mettra gratuitement à disposition des outils de cryptage gratuits.

En attendant, les terroristes se sont déjà repliés sur des outils moins surveillés par la NSA. L'Etat islamique avait privilégié Telegram, une application de communication développée par les frères Durov, deux Russes, qui se disaient peu favorables à l'Occident et se vantaient de n'avoir jamais communiqué d'informations sur leurs utilisateurs.

Sandrine Cassini

Document LEMECO0020151125ebbq0000o

