Edward Snowden a-t-il indirectement contribué aux attentats de Paris ?

Edward Snowden a-t-il indirectement aux attentats de Paris vendredi 13 novembre ?

Des responsables politiques et des membres des services de renseignement internationaux accusent les systèmes de communication chiffrés des géants du web de profiter aux terroristes.

Crédit : DENIS CHARLET / AFP Un gendarme de la Brigade Départementale de Renseignements et d'Investigations Judiciaires (illustration)

Edward Snowden a-t-il indirectement contribué aux fusillades meurtrières qui ont balayé l'est de Paris vendredi 13 novembre ?

Certains acteurs de premier plan du renseignement américain ne sont pas loin de l'affirmer. Sans prononcer le nom de l'ancien analyste de la NSA (l'agence nationale de sécurité américaine), le directeur de la CIA John Brennan a clairement laissé entendre la semaine dernière lors d'une allocution à Washington que ses révélations sur les interceptions massives de communications téléphoniques par la NSA en 2013 avaient participé à faire émerger des failles dans la surveillances des réseaux d'extrémistes.

L'ancien directeur de la CIA James Woolsey ne s'embarrasse pas de ces précautions. Selon lui, Snowden a tout simplement « du sang sur les mains ».

À l'époque, ces révélations avaient poussé le Congrès américain à voter la fin du stockage des métadonnées des appels téléphoniques des citoyens américains par la NSA. Elles avaient surtout encouragé les géants du web à adopter des technologies de chiffrement violemment critiquées par la communauté du renseignement.

Depuis le scandale des pratiques d'écoutes de masse par les États-Unis, la protection des données personnelles est devenu un argument commercial pour les sociétés technologiques auprès d'utilisateurs de plus en plus méfiants des services proposés par les entreprises de la Silicon Valley.

Après le rachat de Whatsapp par Facebook, près de 5 millions d'utilisateurs se sont par exemple rabattus sur le service de messagerie sécurisé Telegram, également plébiscité par les terroristes de Daesh.

Apple a développé des systèmes de sécurité de plus en plus draconiens érigeant ses téléphones en véritables forteresses.

Depuis la fin 2014, les emails, SMS et photos de l'iPhone sont chiffrés et personne, pas même Apple, ne peut y avoir accès.

Selon un expert en cybersécurité cité par Les Échos, « la seule manière d'essayer de les récupérer est de décaper le composant avec de l'acide pour ensuite le passer au microscope ». Une opération qui peut coûter plusieurs millions d'euros.

Dans le même temps, Google, Facebook, WhatsApp, Skype ou Twitter n'ont pas ménagé leurs efforts pour sécuriser les données de leurs abonnés. Si bien qu'il est impossible pour les autorités de lire et d'écouter les conversations sur ces services en dehors de réquisitions judiciaires ou d'un accord avec ces entreprises.

Une loi à l'étude au Royaume-Uni

Les autorités et la communauté du renseignement montent régulièrement au créneau pour réclamer un changement de politique des entreprises technologiques.

Le procureur de Manhattan, Cyrus Vance, a répété à plusieurs reprises qu'il a dû abandonner cette année une centaine d'affaires impliquant des meurtriers, faute d'avoir pu accéder aux données de leurs téléphones.

Le directeur du FBI dénonçait en juillet le chiffrement pratiqué par Whatsapp et les entreprises privées, qui permet, selon lui, à des criminels de se mettre à l'abri de la loi.

Au premier rang de leurs revendications figure la création de clés de chiffrement ou de portes dérobées qui leur donneraient accès aux données des utilisateurs quand la situation l'exigerait.

Le débat est également d'actualité de l'autre côté de l'Atlantique. Après les attentats de janvier à Paris, le premier ministre britannique, David Cameron, s'était publiquement interrogé sur les risques de l'existence de données cryptées auxquelles la police ne peut pas accéder. Il souhaite désormais faire figurer dans l'Investigatory Powers Bill, sorte d'équivalent de la loi renseignement française, l'interdiction des méthodes de chiffrement qui n'incluraient pas de porte dérobée permettant aux autorités munies d'un mandat de justice d'accéder aux informations chiffrées. Une nouvelle législation que le locataire du 10, Downing Street justifie par la nécessité de « ne pas créer une situation dans laquelle les terroristes, les criminels et les ravisseurs d'enfants auraient un espace libre pour communiquer ».

Les géants du web rappellent leur attachement au chiffrement

Les géants du net sont fermement opposés à ce type de mesure. Selon eux, leur mise en place reviendrait à introduire une faille dans leurs programmes. Apple, Microsoft, Google, Samsung, Twitter, Facebook et une cinquantaine d'entreprises technologiques regroupées au sein de l'Information Technology Council ont rappelé dans une lettre ouverte que le chiffrement est un outil de sécurité indispensable pour leurs utilisateurs. « Affaiblir le chiffrement quand on a pour but de l'améliorer n'a aucun sens, estiment-ils. Le chiffrement est un outil de sécurité utilisé tous les jours pour empêcher des criminels de vider nos comptes en banque, pour protéger nos voitures et avions des piratages et pour préserver notre sécurité. (…) Affaiblir le chiffrement ou créer des portes dérobées (…) créerait des vulnérabilités qui pourraient être exploitées par les méchants, ce qui causerait certainement des problèmes physiques et financiers sérieux dans notre société et notre économie ».

La France n'a pas encore pris de position claire sur la question. Mi-août, le procureur de la République de Paris, François Molins, a cosigné une tribune du New York Times avec plusieurs responsables internationaux de la lutte antiterroriste pour appeler les géants du web à changer leur politique de chiffrement pour ne pas affaiblir les capacités d'investigation de la justice contre le terrorisme. Adoptée en juin, la loi Renseignement portée par le gouvernement après les attentats de janvier n'évoque pas précisément la cryptologie. Selon Médiapart, le gouvernement avait l'intention de légiférer mais y a finalement renoncé. C'était avant les attentats de Paris. François Hollande a depuis affirmé devant le Parlement réuni à Versailles qu'il souhaitait adapter l'état d'urgence aux évolutions technologiques, sans donner plus de détails.

Les terroristes n'ont pas attendu Snowden

En attendant, il n'a pas été établi à ce stade de l'enquête que les commandos des attentats de Paris ont utilisé un système de communication crypté pour organiser leurs attaques. Le site d'investigation britannique The Intercept a rappelé récemment que les terroristes et les criminels n'ont pas attendu les révélations de Snowden pour se méfier des voies de communication traditionnelles. Les attentats de New York (2001), Bali (2002), Madrid (2004), Londres (2005), Mumbai (2008) et Boston (2013) peuvent malheureusement en témoigner. Le commanditaire des attentats du 11 septembre, Oussama Ben Laden, s'appuyait par exemple uniquement sur un système de messagers humains par crainte d'être pisté par les services de renseignement, notait le Washington Post. Un système qui lui a permis de naviguer en dehors des radars antiterroristes pendant près d'une décennie.

Réagissez à cet article

Source : http://www.rtl.fr/culture/web-high-tech/apple-google-et-les-geants-du-web-entravent-ils-la-lutte-contre-le-terrorisme-7780616618

PAR BENJAMIN HUE