Les crypto-wars (2/3): une drôle de guerre de quarante ans

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE SAMEDI 30 AVRIL 2016

Martin Hellman, au centre, avec deux étudiants © Service de presse de Stanford

© Reuters

© Reuters

Depuis plusieurs mois, les autorités américaines multiplient les procédures contre Apple pour tenter de lui imposer d'installer sur ses téléphones un *backdoor*, une porte dérobée, leur permettant de déchiffrer plus facilement ses téléphones. La société pour l'instant refuse, mais un projet de loi allant dans ce sens est en cours de préparation au Congrès. Derrière ce bras de fer se cache un conflit entre agences et défenseurs des libertés publiques, né à la fin des années 1970.

>Les crypto-wars (1/3): le chiffrement dans le viseur du gouvernement français

Le débat sur l'usage du chiffrement, et de son éventuelle limitation, n'a pas lieu qu'en France (voir la première partie de notre série). Bien au contraire, c'est une offensive mondiale. Au mois d'août 2015, le procureur de Paris François Molins, deux de ses collègues, un Américain et un Espagnol, ainsi que le préfet de police de Londres signaient **une tribune commune dans le *New York Times*** dénonçant les dangers du chiffrement. *« Au nom des victimes de crimes dans le monde entier, nous demandons si le chiffrement vaut vraiment le coup »*, assenaient-ils. Les auteurs donnaient l'exemple précis d'un fait divers dans lequel les enquêteurs n'auraient pas pu déchiffrer le contenu d'un téléphone retrouvé sur les lieux du crime.

Mais surtout, ils dénonçaient la décision prise, au mois de septembre 2015, par Google et Apple de chiffrer leurs systèmes pour smartphones : *« Les nouvelles pratiques de chiffrement d'Apple et Google rendent plus difficile la protection de la population contre les crimes*, affirmaient les magistrats et le préfet. *En l'absence de coopération d'Apple et Google, les régulateurs et législateurs de nos pays doivent trouver un moyen approprié d'équilibrer le gain minime lié au chiffrement entier des systèmes et la nécessité pour les forces de l'ordre de résoudre les crimes et poursuivre les criminels. »*

Après les attaques du 13-Novembre à Paris et la tuerie de San Bernardino, aux États-Unis en décembre 2015, la polémique n'a fait qu'enfler. Elle s'est transformée en conflit ouvert le 9 février, lorsque le FBI annonce être en possession d'un iPhone appartenant aux deux terroristes de San Bernadino mais qu'il est dans l'incapacité de le déverrouiller en raison du nouveau système de chiffrement mis en place par Apple. Mais au lieu de demander simplement la transmission des données en question, le FBI exige de la firme à la pomme qu'elle installe un *backdoor* dans ses téléphones en développant un logiciel qui lui permettrait d'accéder directement aux données.

Apple entame alors un bras de fer avec les autorités américaines en contestant publiquement la demande du FBI. Celui-ci saisit un juge et obtient, le mardi 15 février, un ordre intimant à la société d'installer le *backdoor* demandé. Le lendemain, le PDG de la société, **Tim Cook, prend la plume** pour expliquer à ses clients qu'il ne se pliera pas à cette injonction. Le bureau fédéral lui répond le 19 février en saisissant un tribunal afin d'obtenir l'application forcée de l'ordre émis le 15 février.

© Reuters

L'affaire fait la une des journaux du monde entier et alimente notamment le débat en cours en France (voir la première partie de notre série). Devenu le héraut de la défense de la vie privée, Apple reçoit de nombreux soutiens de la part d'associations de défense des droits de l'homme et d'universitaires. La Silicon Valley fait également bloc. Les géants du Net, dont Edward Snowden a pourtant largement exposé la complicité avec la NSA, **déposent même devant le tribunal un *brief* de soutien** signé par Amazon, Facebook, Google, Microsoft, Snapchat ou encore Yahoo!.

L'affaire connaît finalement un étrange dénouement. Le 21 mars, le gouvernement demande une suspension des poursuites contre la société, affirmant avoir trouvé un moyen de débloquer le téléphone. Une semaine plus tard, elles sont définitivement abandonnées. La presse, et notamment **le journal israélien *Yedioth Aharonot***, affirme dans un premier temps que le FBI aurait eu recours à une société israélienne, Cellebrite. Mais le 12 avril, **le *Washington Post* révèle** de son côté que le gouvernement aurait en fait payé des *hackers* ayant découvert une vulnérabilité déjà existante dans le système d'Apple. Et, **selon un calcul de Reuters** fondé sur une récente déclaration du directeur du FBI James Comey, le gouvernement aurait payé ces *hackers* plus d'un million de dollars.

Le dossier n'en est pas pour autant clos. Mis en cause par les révélations d'Edward Snowden, les géants du Net n'ont cessé depuis deux ans de tenter de regagner la confiance des internautes, et la défiance vis-à-vis des autorités semble devenue un argument marketing à part entière.

Le 31 mars, le service de messagerie instantanée le plus populaire au monde Whatsapp, utilisé par un milliard de personnes, annonçait une mise à jour de son application afin d'introduire un chiffrement *« de bout en bout »* et *« activé par défaut et constamment »*. **Dans une note de blog** publiée le 5 avril, les deux fondateurs, Jan Koum et Brian Acton, font explicitement référence au débat sur le chiffrement. *« Bien que nous ayons conscience que l'important travail des forces de l'ordre est de protéger les individus, les tentatives d'affaiblir le chiffrement risquent d'exposer les informations des gens et de les rendre accessibles aux cybercriminels, pirates et aux États voyous »*, expliquent-ils. Le 19 avril, son concurrent Viber, qui revendique 711 millions d'utilisateurs, **faisait à son tour une annonce similaire**.

Parallèlement, au Congrès américain, deux importants sénateurs de la commission renseignement ont déposé un projet de loi transpartisan visant à imposer aux entreprises de *« fournir dans un délai raisonnable des informations intelligibles ou des données, ou une assistance technique appropriée pour obtenir de telles informations »*. **Les États de Californie et de New York** envisagent, eux, de tout simplement interdire la vente d'équipements chiffrés ne pouvant être déverrouillés par les forces de l'ordre.

La bataille pour le chiffrement ne fait donc que commencer. Elle ne survient pas à n'importe quel moment. Ce débat émerge bien entendu, et tout d'abord, à la suite des attaques terroristes qui ont frappé l'Europe ces deux dernières années. Mais il intervient également un peu plus de deux ans après les révélations d'Edward Snowden, que certains semblent avoir déjà oubliées. Alors que certains dénoncent des systèmes de chiffrement apparemment inviolables, l'ex-employé de la NSA avait décrit une tout autre situation : des systèmes déjà pervertis par les agences qui n'hésitaient pas à qualifier les utilisateurs d'iPhone de *« zombies »*.

La main invisible de la NSA

Comment expliquer ce décalage ? Tout d'abord par le fait que cette bataille autour du cas d'Apple s'inscrit dans le cadre d'une guerre bien plus large, débutée il y a une quarantaine d'années, et connue sous le nom de **« crypto-war »**. Aux États-Unis, la cryptologie, l'art de dissimuler et de décrypter des informations, n'est entrée dans l'ère électronique que durant la Seconde Guerre mondiale au sein de l'armée américaine, notamment grâce au travail d'Alan Turing, popularisé en 2014 dans le film ***The Imitation Game***.

Dans un premier temps, toutes les recherches sur le sujet sont donc effectuées par la NSA. Durant la guerre froide, l'usage de la cryptologie est ainsi exclusivement militaire. Le but des États-Unis, et de leurs alliés, est alors d'empêcher tout transfert de cette technologie naissante vers le bloc soviétique. Réunis au sein du CoCom (Comité de coordination pour le contrôle multilatéral des exportations), les ex-Alliés imposent un contrôle de toute exportation d'armes ou de technologie sensible. Mais à partir des années 1960, l'informatisation de l'économie va peu à peu bouleverser la donne. Avec la mondialisation croissante de la finance, les acteurs économiques vont

très vite demander de disposer, eux aussi, d'outils pour sécuriser les transactions financières de plus en plus immatérielles.

Ironie du sort, ce sont les autorités elles-mêmes, et plus particulièrement la NSA, qui seront à l'origine de la mise à la disposition du grand public des outils de chiffrement informatique et de la diffusion massive de la cryptologie moderne. Au début des années 1970, le Bureau national des standards (NBS), chargé de déterminer et valider tout type de normes officielles en vigueur aux États-Unis, lance un appel d'offres afin d'unifier la sécurisation des flux de données sensibles collectées de plus en plus massivement par les administrations américaines. Après consultation de la NSA, la NBS lance en mai 1973 le concours pour la création d'un système de chiffrement qui servirait de standard national : **le Data Encryption Standard**, ou DES.

Seule la société IBM a les capacités techniques de répondre à un tel défi. En 1975, le géant de l'informatique propose une première version du DES, fondé sur un algorithme développé durant deux ans par ses ingénieurs. Celle-ci sert ensuite de base à deux années de travaux durant lesquelles naissent, déjà, les premières suspicions autour de l'influence, alors seulement supposée, de la NSA sur ces travaux. Ces craintes ont tout d'abord été exprimées par des chercheurs, pionniers dans le domaine de la cryptologie informatique. Elles seront, au fil des années, confirmées et attestées par plusieurs témoignages et documents déclassifiés. En résumé, la NSA n'avait pas réellement installé de *backdoor*, de porte dérobée, dans le DES mais avait obtenu d'IBM quelques modifications afin de pouvoir le briser plus facilement.

Concrètement, il a été avéré que l'agence a obtenu de la société qu'elle réduise la taille de la clef. Celle-ci est utilisée par les utilisateurs pour chiffrer ou déchiffrer les messages et sa taille est exprimée en bit. Plus une clef est longue, plus le déchiffrement du message par la « force brute » d'un ordinateur sera difficile. À l'origine, les ingénieurs d'IBM avaient prévu un DES avec une clef de 64 bits. La NSA demandait de son côté qu'elle ne soit que de 48 bits. Un compromis a été trouvé avec une clef affaiblie à 54 bits. Des chercheurs ont également repéré de mystérieuses « S-boxes » (boîtes de substitution en français), un des composants de l'algorithme central dans le chiffrement du message dont le rôle n'a jamais été clairement établi.

Malgré les critiques et les suspicions qui s'exprimaient déjà, le DES a été validé en tant que standard fédéral au mois de novembre 1976. Cette première tentative de définition d'une norme comporte en elle toutes les tensions et les paradoxes de cette discipline. Née dans des laboratoires militaires, la cryptographie moderne reste la création d'une communauté de chercheurs souvent sensibilisés aux questions de protection de la vie privée. *« Quand IBM a soumis le DES comme standard, personne en dehors de la NSA n'avait l'expertise pour l'analyser »*, résumait, **dans un article de 2004** rendant hommage aux pionniers de la cryptologie moderne, Bruce Schneier, un des experts américains en sécurité informatique les plus réputés. *« Les changements de la NSA ont provoqué un tollé parmi les quelques personnes qui faisaient attention (…). Mais du tollé vint la recherche,* écrivait-il. *Il n'est pas exagéré de dire que la publication du DES a créé la discipline académique moderne de la cryptographie. »*

Un des meilleurs exemples de cette confrontation, pleine d'ambiguïtés, entre militaires et universitaires est sans doute l'histoire unissant Martin Hellman, chercheur à l'université de Stanford, et le vice-amiral Bobby Ray Inman, nommé à la tête de la NSA durant l'été 1977. Chercheur en génie électrique, Martin Hellman fait partie des premiers à se pencher sur le DES préparé par IBM et la NSA. En novembre 1976, il publie, avec un de ses étudiants Whitfield Diffie, un article fondateur : ***« New Directions in Cryptography »*** (*« De nouvelles directions en cryptographie »*). *« L'article introduisait les principes qui forment aujourd'hui les bases de la cryptographie moderne »*, explique le chercheur Henry Corrigan-Gibbs dans un article très informé **publié en novembre 2014 par le *Stanford Magazine*** et revenant en détail sur l'affaire. *« Sa publication*

a légitimement provoqué un grand émoi parmi les ingénieurs en génie électrique. » Mais la NSA, elle, était *« apoplectique »*. *« Le fait que Hellman et ses étudiants aient défié le monopole domestique maintenu depuis longtemps par le gouvernement sur la cryptographie ennuyait profondément beaucoup de monde au sein de la communauté du renseignement. »*

Martin Hellman, au centre, avec deux étudiants © (Service de presse de Stanford)

Concrètement, la NSA craignait que les travaux de Hellman ne permettent à des organisations non militaires de développer leurs propres techniques de chiffrement, sur lesquelles l'agence n'aurait pas la main. Mais surtout, le chercheur a prévu de présenter les résultats de ses travaux lors du Symposium international sur la théorie de l'information qui doit se tenir le 10 octobre 1977 à la Cornwell University. Dans les mois qui précèdent, Hellman et ses collaborateurs sont la cible de pressions de plus en plus précises. Au mois de juillet, l'Institute of Electrical and Electronical Engineers (IEEE), qui avait publié l'étude de Hellman, reçoit une mystérieuse lettre, signée par un certain J.A. Meyer, les menaçant à mots couverts de poursuites. L'article, en démocratisant le chiffrement, serait équivalent à une mise à disposition, et donc à une exportation, d'une technologie encore considérée comme militaire. *« Ces armes technologiques modernes, disséminées de manière incontrôlée, pourraient avoir des effets plus qu'académiques »*, prévenait l'auteur.

Ce courrier, qui aurait pu passer inaperçu, suscite de vives inquiétudes chez de nombreux chercheurs. D'autant plus que, peu de temps après, deux journalistes **du magazine *Science* révèlent** que le mystérieux J.A. Meyer n'est autre qu'un employé de la NSA. Martin Hellman comprend alors les risques qui pèsent sur lui et sur ses étudiants et commence à préparer sa défense avec l'avocat de Stanford, en vue de la tenue du symposium et de l'ouverture d'éventuelles poursuites.

Parallèlement, la publication des révélations de *Science* sur les pressions de la NSA intervient à un moment charnière pour l'agence. La lettre de menaces de J.A. Meyer a en effet été écrite le jour même de l'entrée en fonctions d'un nouveau directeur : le vice-amiral Bobby Ray Inman. Dans le *Stanford Magazine*, le militaire raconte s'être d'emblée trouvé plongé dans *« un énorme tumulte médiatique »*. Il explique également n'avoir pas compris pourquoi des scientifiques civils s'intéressaient tant à une technologie alors uniquement militaire. *« Les autres personnes à l'époque qui achetaient du chiffrement pour l'utiliser étaient les vendeurs de drogue »*, explique-t-il.

Inman veut comprendre ce qui motive ces jeunes chercheurs chevelus et barbus. Il se rend en personne en Californie pour les rencontrer sur leur terrain, les campus de Berkeley ou de Stanford. Il s'entretient bien entendu avec Martin Hellman. Les deux hommes deviendront même amis par la suite. De ces discussions, le nouveau patron de la NSA comprend que la cryptologie a déjà commencé à échapper à la mainmise militaire. Les entreprises, le monde de la finance réclament déjà des moyens de sécuriser leurs échanges. Et cette génération de chercheurs est bien déterminée à offrir au grand public, au nom de la liberté d'expression, les moyens de protéger ses communications. *« Il y a tout un nouveau monde qui émerge là-bas, où il y aura besoin de cryptographie. Et elle ne sera pas fournie par le gouvernement »*, écrit-il.

Les combats des pionniers du chiffrement

Martin Hellman a finalement pu présenter son travail lors du symposium sans être inquiété. Mais Inman continue à penser que son agence doit garder le contrôle notamment, et déjà, pour des raisons d'espionnage international. *« Nous nous inquiétions que des pays étrangers ramassent et utilisent la cryptographie, ce qui rendrait excessivement difficile de déchiffrer et de lire leur trafic »*, raconte-t-il au *Stanford Magazine*. À son retour, il forme au sein de la NSA un panel chargé d'étudier la question. Celui-ci a répondu en proposant trois options : *« a- Ne rien faire ; b- Chercher une nouvelle législation pour imposer un contrôle gouvernemental supplémentaire ; c- Essayer des moyens non législatifs tels que la conformité volontaire commerciale et académique. »*

Pour Inman, la première solution était inenvisageable. Il a donc, dans un premier temps, envisagé la deuxième. Mais celle-ci s'est vite avérée impossible en raison de l'opposition du Congrès, alors lancé dans un processus de libéralisation du commerce extérieur, et des universitaires bien décidés à publier leurs recherches quoi qu'il en coûte. Ne restait donc plus que la troisième option. Si la diffusion du chiffrement est impossible à empêcher, autant tout faire pour en contrôler la diffusion à sa source, en influant sur le travail des universitaires et des fabricants.

La NSA met tout d'abord en place un système de relecture volontaire des articles scientifiques avant leur publication. Celui-ci s'est vite retrouvé débordé par l'explosion de l'usage du chiffrement et a disparu au bout d'une dizaine d'années. Mais le gouvernement américain dispose d'un autre levier pour influer sur l'évolution de la cryptologie : le financement de la recherche. Dès 1977, la NSA propose à la Nation Science Foundation (NSF), distribuant des bourses de recherche, de l'aider à sélectionner les projets en fonction de leurs *« mérites techniques »*. Malgré les interventions de l'agence qui relit les projets avant leur sélection, NSF semble avoir conservé une certaine indépendance. Mais la NSA dispose d'une influence beaucoup plus directe sur certaines autres entités du gouvernement, connues pour financer de très nombreux projets scientifiques : le Darpa (Agence pour les projets de recherche avancée de défense), le Bureau de recherche navale ou encore le Bureau de recherche de l'armée.

© Reuters

Le DES, lui, ne survivra pas aux coups de boutoir des chercheurs. Pour prouver définitivement son manque de sécurité, un groupe de scientifique lance, en 1997, le premier *« DES Challenges »*, une série de défis visant à briser l'algorithme. La même année, le NBS, rebaptisé National Institute of Standards and Technologie (Nist), commence à travailler sur un nouveau standard. Pour éviter de nouvelles suspicions, un concours international est cette fois lancé. Il est remporté par deux cryptographes belges, Joan Daemen et Vincent Rijmen. Le 26 mai 2002, **l'Advanced Encryption Standard** (AES) devient officiellement la nouvelle référence, en remplacement du DES. Bien que la NSA ait, cette fois encore, relu l'intégralité des projets sélectionnés, l'AES est cette fois considéré comme relativement sûr.

Un autre héros des crypto-wars s'appelle Philip Zimmermann. En 1991, cet ingénieur informaticien et militant antinucléaire de longue date a mis au point son propre logiciel de chiffrement, fondé sur un algorithme de sa création. **Baptisé PGP, pour « *pretty good privacy* »**, celui-ci est destiné à la communauté des militants pacifistes et activistes politiques qui commencent à utiliser un Internet encore balbutiant pour discuter et échanger des documents. Le problème est que la clef utilisée par PGP est d'une longueur de 128 bits. Or, les lois américaines sur l'exportation considéraient encore comme arme toute solution de chiffrement dont la clef dépassait les 40 bits. La diffusion de PGP est dans un premier temps confidentielle. Philip Zimmermann envoie le logiciel à trois amis pour qu'ils le postent sur de groupes Usenet, ancêtres des forums. À l'un deux, il prend la précaution de demander de préciser la mention *« US only »*.

Évidemment, « PGP » ne restera pas longtemps cantonné à quelques réseaux privés américains. En quelques mois, il se propage sur le réseau et dans le monde entier. En février 1993, les autorités américaines ouvrent une enquête pour *« exportation d'arme sans autorisation »*. Pour contourner la loi américaine, Philip Zimmermann trouve une parade. En 1995, il publie l'intégralité du code source de PGP dans un livre édité par le MIT. Il suffisait ensuite aux acheteurs de scanner chaque page et d'utiliser un logiciel pour reconstituer PGP sous sa forme originale. **En préface de son livre**, composé de lignes de code, Phil Zimmermann revendique ouvertement le fait de braver les autorités : *« Pourquoi publier un livre complet (et un gros) composé principalement d'un ennuyeux code pour un programme informatique ? Eh bien, il y a de très bonnes raisons. Elles concernent nos libertés civiles. »* L'argument avancé

par Zimmermann pour défier une nouvelle fois les autorités américaines est que le livre, contrairement à un logiciel informatique, échappe à la loi sur la réglementation des exportations et bénéficie même de la protection du sacro-saint premier amendement sur la liberté d'expression.

À la même époque, la toute jeune société Netscape, qui sera principalement connue par la suite pour son navigateur, met sur le marché son propre protocole de chiffrement : **le Secure Sockets Layer** (SSL). Contrairement à PGP, il s'agit cette fois d'un produit commercial destiné à être décliné pour sécuriser les mails, les fax, l'échange de données entre serveurs… La clef de SSL est elle aussi de 128 bits et tombe donc sous le coup de la loi américaine sur les exportations. Mais Netscape n'est pas prête à se lancer dans un bras de fer avec les autorités. La société décide de commercialiser deux versions de SSL : une « marché US », avec la clef originale de 128 bits, et une « internationale », avec une clef affaiblie à 40 bits.

Très tôt, la NSA s'intéresse aussi aux communications téléphoniques et au marché des téléphones portables, encore émergent. En 1993, elle développe en secret une puce électronique baptisée **« *clipper chip* »** et équipée d'un algorithme lui aussi de sa fabrication. Le but de l'agence est d'imposer à tous les fabricants d'installer cette puce sur leurs téléphones. L'algorithme, lui, est censé chiffrer les communications. Mais pour cela, il crée une clef qui ne sera pas détenue par l'utilisateur mais stockée dans une sorte de séquestre géant centralisant l'ensemble des clefs. La NSA disposerait alors, à portée de clic, des moyens de déchiffrer l'ensemble des communications. Le projet a évidemment suscité un véritable tollé chez les défenseurs des libertés publiques et il a été définitivement abandonné en 1996.

Les autorités américaines se rendent compte qu'elles sont face à un imbroglio. Comme l'avait prédit Bobby Ray Inman après sa visite en Californie, un « nouveau monde » a émergé. Le chiffrement s'est répandu un peu partout dans les universités américaines et étrangères. Mais surtout, il est devenu un enjeu commercial majeur pour les sociétés américaines. La version « internationale » de SSL pouvait ainsi être déchiffrée par un ordinateur personnel en seulement quelques jours.

Parallèlement, les chercheurs et défenseurs des libertés publiques n'ont pas relâché la pression. En 1995, **Daniel J. Bernstein**, étudiant à l'université de Berkeley, souhaite publier dans un article scientifique le code source d'un système de chiffrement qu'il a créé, Snuffle. Il se lance alors dans une bataille juridique de plusieurs années contre la loi sur les exportations. Il remporte une première victoire dès 1996, confirmée en appel en 1999, dans un jugement fondamental qui reconnaît que le code source d'un logiciel relève bien de la liberté d'expression, protégée par le premier amendement de la Constitution.

Toujours en 1996, débute une autre affaire. Professeur en droit à la Case Western Reserve University, dans l'Ohio, et hacktiviste, **Peter Junger** souhaite introduire dans son programme des cours de droit de l'informatique. Mais pour cela, il prévoit d'initier ses étudiants au chiffrement. Or, parmi ceux-ci figurent plusieurs étrangers. Et si l'on suit une interprétation stricte de la loi, le simple fait de donner par oral à un non-Américain des détails sur un logiciel de chiffrement soumis à autorisation est interdit. Junger affirme que la législation l'oblige à refuser des étudiants étrangers et viole le premier amendement. Son combat se soldera, en 2000, par une nouvelle décision d'une cour fédérale d'appel qui confirme que le code source d'un logiciel relève bien de la liberté d'expression.

De son côté, Phil Zimmermann ne sera finalement jamais jugé. PGP est depuis devenu la référence en matière de solution libre de chiffrement et a servi de base à de nombreux autres logiciels, **comme GPG**, très utilisé pour le chiffrement de mails. Sous pression des militants, mais surtout des entreprises, les autorités américaines ont peu à peu assoupli progressivement les règles sur les exportations, leur assurant ainsi la domination du marché. Dès 1996, Bill Clinton ordonne le retrait du chiffrement de la liste des « armes et munitions » soumises à autorisation. Son

exportation est désormais gérée par le département du commerce, qui a encore assoupli les règles lors d'une réforme en 2000.

Mais ce *happy end* n'a pas manqué de relancer la paranoïa de certains, pour qui cette apparente clémence ne serait que le signe de la main invisible de la NSA. En 2000, peu après les révélations sur le système d'espionnage mondial « Echelon », le député Arthur Paecht avait ainsi été chargé **d'un rapport faisant le point sur les capacités des États-Unis** en matière de surveillance internationale. La question du chiffrement, et le cas de PGP, sont bien entendus évoqués. *« Les attaques qui ont été menées par la NSA sur le plan judiciaire contre les logiciels Pretty Good Privacy ont cessé et la dernière version proposée a reçu l'aval des autorités américaines »*, relevait le rapporteur, avant d'ajouter : *« Il est donc à craindre que ces logiciels ne soient plus aussi libres que par le passé et que des accords aient été conclus entre les agences fédérales américaines et le concepteur du système. »*

"Bullrun" relance les crypto-wars

Au début des années 2000 et jusqu'à il y a encore quelques années, un équilibre semblait cependant avoir été trouvé au sein des « crypto-wars ». Même si personne ne doute que la NSA ait pu continuer à tenter d'influer en sous-main, les outils de chiffrement se sont propagés dans le monde entier. Les exportations, elles, dépendent du département du commerce et sont régies, au niveau international, par l'arrangement de Wassenaar signé par une quarantaine de pays et interdisant la vente de certaines technologies à des États ne respectant pas les droits de l'homme.

Mais cette trêve va voler en éclats en 2013, sous le coup des révélations d'Edward Snowden. Le 5 septembre, le *Guardian*, le *New York Times* et ProPublica révèlent **l'existence du programme « Bullrun »** dont le but n'est autre que de *« battre le chiffrement »*. Pour cela, la NSA et son homologue britannique le GHCQ ont lancé une campagne tous azimuts : progrès techniques, pressions sur les fabricants et les chercheurs, installation de « *backdoors* »… Peu de détails techniques ont été dévoilés sur *Bullrun*, les journaux ayant accepté de censurer certaines informations à la demande des autorités américaines. Mais l'on sait qu'il s'agit du programme le plus richement doté de la NSA, avec un budget annuel de 250 millions de dollars par an. Un des documents fait état d'actions vis-à-vis de sociétés *« américaines et étrangères »* visant à *« secrètement influencer »* le design de leurs produits. La presse cite en particulier un algorithme homologué par le NIST en 2004, le Dual EC, qui serait équipé d'un *backdoor*. Plus généralement, la NSA et le GHCQ auraient très fortement amélioré leurs capacités de déchiffrement. Un document notamment évoque une percée technique capitale durant l'année 2010, ayant permis l'exploitation d'une *« grande quantité »* de données.

Dans un domaine où la paranoïa relève souvent de la simple prudence, ces révélations ont relancé les *crypto-wars* en sommeil. Cette fois, ce sont les grandes sociétés du Net qui se présentent en fers de lance de la contestation. Mis en cause par de nombreux documents d'Edward Snowden pour leur complicité avec la NSA, les géants du Net se sont depuis tous lancés dans des opérations de communication sur la sécurisation de leurs réseaux. Google, Facebook, Twitter… tous ont dénoncé les ingérences des autorités et annoncé des mesures de chiffrement.

Ce fut également le cas d'Apple. Certains, d'ailleurs, s'étonnent de voir aujourd'hui la société endosser dans son conflit avec le FBI le costume du défenseur de la vie privée alors que, dans un document d'Edward Snowden, la NSA qualifiait ses utilisateurs de *« zombies »*. **Dans un article du 3 septembre 2013**, le *Spiegel* détaillait en effet les techniques utilisées par la NSA pour récupérer les données stockées sur des smartphones. Dans une présentation, l'agence raille même Apple et son fondateur Steve Jobs, à travers une référence à la publicité de lancement du premier ordinateur de la marque, le Macintosh, en 1984. *« Qui aurait cru, en 1984, que ça deviendrait Big Brother… et que les zombies seraient des utilisateurs payants ? »*

Le combat entre Apple et le FBI ne serait-il qu'un jeu de dupes ? Interrogé au début de mois de mars sur l'affirmation selon laquelle le fabricant serait le seul à pouvoir déverrouiller ses téléphones, le lanceur d'alerte **Edward Snowden a eu cette réponse** : *« Respectueusement, ce sont des conneries. »*

Edward Snowden sur le chiffrement de l'iPhone (A partir de 30'00)

En tout cas, l'affaire du téléphone de San Bernardino s'inscrit bien dans un contexte bien plus large. La société a en effet annoncé avoir reçu au total une douzaine de demandes du même type émanant de cours fédérales. L'une d'entre elles vise un iPhone saisi dans le cadre d'une affaire de drogue dans l'État de New York. Cette fois encore, le FBI affirme ne pas être en mesure de déverrouiller l'appareil et exige d'Apple qu'il modifie son logiciel. Mais cette fois, la société a gagné en première instance. Le 29 février, le juge James Orenstein a rejeté la demande au motif que *« les implications de la position du gouvernement sont d'une si grande portée (…) qu'elle conduirait à produire des résultats absurdes inadmissibles »*.

Le vendredi 8 avril, le bureau du procureur de New York a annoncé que le gouvernement avait fait appel de cette décision. Vendredi dernier, l'avocat d'Apple a envoyé au juge ses arguments : le FBI ayant réussi à débloquer le téléphone de San Bernardino, il n'y a aucune raison de l'aider à déverrouiller celui de Brooklyn. Mais le Bureau affirme de son côté qu'il s'agit de deux modèles différents et que la méthode utilisée sur l'un ne fonctionne pas sur l'autre.

La bataille se poursuit donc. Mardi 19 avril, **le Congrès américain entamait ses auditions** en vue de préparer le projet de loi transpartisan sur le chiffrement. Devant les parlementaires, la directrice adjointe du FBI en charge des technologies et de la science, Amy Hess, a réaffirmé que son agence avait besoin d'une collaboration pleine et entière des entreprises, même si le Bureau a été capable de déverrouiller l'iPhone de San Bernardino. *« Ce type de solutions que nous pouvons employer requiert beaucoup de ressources spécialisées hautement qualifiées dont nous ne disposons pas toujours immédiatement »*, a-t-elle affirmé.

De son côté, le représentant d'Apple, Bruce Sewell, a une nouvelle fois affirmé que les forces de l'ordre disposaient de nombreux moyens pour récupérer des informations, sans avoir à imposer des *backdoors* aux fabricants. Un fait confirmé à Mediapart par la cryptologue Anne Canteaut (voir son interview). *« Sur l'ensemble des algorithmes existants, il y en a une quantité qui n'ont pas encore été cassés. Mais cela ne veut pas dire qu'ils sont sûrs. Il n'existe aucun algorithme qui soit sûr dans l'absolu »*, explique-t-elle. Mais surtout, elle souligne que *« le débat est biaisé car il se focalise sur un micro-aspect du problème. En fait, c'est assez peu le chiffrement qui est mis en cause dans les attaques, mais davantage tout ce qu'il y a autour du chiffrement. Ces dernières années, les possibilités d'accès aux données ont été démultipliées. »* Ainsi, concernant l'iPhone de San Bernardino, on a *« beaucoup parlé des communications bloquées dans le téléphone. Mais assez peu du fait qu'elles ne représentaient que cinq jours. Tout le reste avait été synchronisé par les services d'Apple et stockés sur des serveurs. Et là, le FBI y a bien eu accès. Le fait qu'Apple stocke les communications de ses utilisateurs aurait dû tout de même susciter quelques réactions… »*.

En somme, *« Apple se refait une virginité à peu de frais ! »*, résume Anne Canteaut. Transformer Apple, Whatsapp, Google ou Facebook en défenseurs des libertés serait en effet oublier que ces sociétés sont bien du côté des surveillants. Outre leur collaboration directe avec les agences américaines, les documents d'Edward Snowden ont montré à quel point elles étaient indispensables au dispositif de surveillance mondial mis en place par les États-Unis, notamment grâce à l'utilisation massive de données et de métadonnées générées par leurs utilisateurs. Devant le Congrès américain, Bruce Sewell n'a d'ailleurs pas manqué de le rappeler aux parlementaires : *« Comme vous avez pu l'entendre de nos collègues des forces de d'ordre, ils ont la perception que le chiffrement les isole des informations »*, a expliqué le représentant

d'Apple. *« Mais les technologues et les experts en sécurité nationale ne voient pas le monde de cette manière. Nous voyons un monde riche en données qui semble plein d'informations. Informations que les forces de l'ordre peuvent utiliser pour résoudre – et prévenir – les crimes. »*

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.