FBI-iPhone : Un décryptage et un débat sans réponses

Dans la nuit, l'information est tombée : le FBI a réussi à décrypter l'iPhone d'un des responsables de l'attaque terroriste de San Bernardino sans l'aide d'Apple. Cette issue attendue a viré du feuilleton judiciaire à l'affrontement symbolique entre les sociétés IT (se posant en garant des libertés individuelles) et l'Etat (accusé de s'immiscer de plus en plus dans la vie privée des personnes).

Sans donner plus de détails sur son intervention, le FBI a sans doute été aidé dans son entreprise par un tiers. La presse, la semaine dernière, s'est faite l'écho d'un partenariat avec la société israélienne Cellebrite. De même les spécialistes de la sécurité s'étaient étonnés de la faiblesse du FBI à percer les défenses de l'iPhone incriminé. Pour autant, il existe plusieurs options logicielles et hardware pour mener à bien cette opération. Même John McAfee s'est promis de manger sa chaussure en cas d'échec, finalement évité par le décryptage du FBI.

Apple a-t-il le droit de refuser la contrainte judiciaire ?

Avec cette annonce de l'agence fédérale, les poursuites judiciaires contre Apple s'éteignent avec le sentiment de chaque côté d'un débat gâché et non terminé. Cette affaire aura mis en exergue plusieurs questions aujourd'hui sans réponses. La première interrogation est celle de la légitimité, est-ce que le gouvernement est en droit de demander à une société IT l'accès à un équipement technologique pour mener des enquêtes ? Dans le même temps, est-ce que cette même société est légitime à refuser cette demande et sur quelle base juridique ?

Dès le début de l'affaire, les juristes de chaque camp ont donné leurs arguments. Pour l'Etat, la demande d'accéder à l'iPhone était une décision de justice et non pas une demande extra-judiciaire, Apple avait donc l'obligation de s'y conformer. Pour Apple, cette coopération forcée est une atteinte à la vie privée de ses clients qui lui font confiance pour garantir la sécurité de leurs vies privées. Tim Cook en personne a défendu à plusieurs reprises cette position et a rallié une majorité d'entreprises IT à ses vues. Le patron d'Apple était prêt à la bataille en souhaitant même que le débat soit porté devant la Cour suprême. En refermant la parenthèse judiciaire, les deux parties privent l asociété civile d'une jurisprudence qui aurait pu faire avancer ces questions d'immixtion dans la vie privée, quelles sont les frontières, quelles sont les exigences pour y déroger, etc.

Doit-on légiférer sur ce cas spécifique ?

Si les débats se sont focalisés sur l'aspect juridique, ils se sont vites déplacés sur le plan politique. Un déplacement souhaité par Apple qui a réclamé à maintes reprises que les représentants de la Nation se saisissent du sujet et légifèrent dessus pour clarifier la situation. Le gouvernement américain est resté inflexible aux demandes de la firme de Cupertino, allant même jusqu'à faire miroiter la menace de l'obliger à fournir le code source d'iOS, ainsi que la clé de chiffrement privée

d'Apple (en se basant sur le précédent Lavabit). Les candidats à la primaire pour l'élection présidentielle américaine ont été invités à prendre parti sur cette affaire. Boycott d'Apple et des iPhone pour Donald Trump, compréhension des deux points de vue pour Hillary Clinton et Bernie Sanders sans prises de position tranchées. Même ce débat a eu une résonnance outre-Atlantique avec des questionnements sur le processus de ratification de Privacy Shield (successeur désigné du Safe Harbor). En France aussi l'affaire secoue le Parlement. Un député PS a déposé un amendement où tout refus d'assistance de la part de sociétés comme Apple ou Google – concepteur d'Android – se traduirait par une amende d'un montant d'un million d'euros. Un autre député, Eric Ciotti a réclamé l'interdiction de commercialisation des technologies en cas de non collaboration avec la justice dans le cadre des affaires terroristes. L'amendement a été écarté de justesse.

Sécurité renforcée des terminaux et des logiciels

Enfin, la dernière interrogation porte sur l'aspect technique du conflit et sur le chiffrement en particulier. D'abord, il faut souligner que la requête du FBI est consécutive d'une erreur de ses services qui ont perdu les identifiants iPhone du tueur. En conséquence, Apple aurait dû créer une version customisée d'iOS afin de contourner certaines sécurités de l'iPhone. Pour la firme de Cupertino, il s'agit ni plus ni moins d'installer une backdoor qui aurait pour conséquence de fragiliser les mesures de sécurité avec un risque qu'à terme des cybercriminels puissent utiliser ces failles. La levée de bouclier ne s'est pas faite attendre y compris par les spécialistes du chiffrement. Ainsi, Ron Rivest (le R de RSA) précise que « *le chemin vers l'enfer commence avec une backdoor* ». Moxie Marlinspike est plus prophétique : « *De façon détournée, ils nous demandent de préparer un monde où cela serait possible. Et ce n'est pas un monde dans lequel j'ai envie de vivre.* » D'autres voix se sont fait entendre comme l'ENISA qui est très critique sur le contournement du chiffrement.

Conséquence de cette bataille, les acteurs de l'IT ont décidé de renforcer la sécurité de leurs produits et de leurs solutions. Apple en tête a annoncé le recrutement du développeur de Signal (messagerie sécurisée) pour renforcer l'iPhone. Tim Cook entend mobiliser ses troupes pour combattre « *l'équivalent d'un cancer* » et donc prévoit d'améliorer la sécurité d'iOS. Sur la partie messagerie, Google, Microsoft et Yahoo ont proposé un nouveau protocole de messagerie STMP baptisé STS (Strict Transport Security). Google en a profité pour dresser dans son rapport sur la transparence un état des lieux sur HTTPS.

Au final, l'affaire FBI contre Apple a montré les limites de la justice face à la volonté d'un industriel à ne pas s'y soumettre quelles que soient les raisons invoquées (légitimes ou pas). Une posture qui n'est pas sans rappeler celle de Microsoft face au gouvernement américain qui veut obtenir des données présentes dans un Cloud de la firme en Irlande. Elle a forcé les politiques à se saisir du problème avec pour ambition de réformer et d'adapter les lois aux exigences de sécurité nationale face aux nouvelles technologies. Enfin, elle a poussé à son paroxysme le débat sur le chiffrement qui empoisonne depuis plusieurs mois les relations entre les agences de renseignements, le gouvernement et les acteurs IT. Si le décryptage de l'iPhone a mis fin à la procédure, les débats vont rester, et c'est finalement un mal pour un bien.

A lire aussi :

iOS 9.3 vous avertit si votre patron surveille votre iPhone

Déblocage des iPhone : les soutiens d'Apple, de New York à San Bernardino

Crédit Photo : wk1003mike-Shutterstock