Chiffrement : la Chine ouvre la boîte de Pandore

Comme nous le laissions entendre le 23 décembre dernier, la Chine a voté dimanche 27 décembre une loi antiterroriste qui fait peser de nouvelles contraintes sur les fournisseurs de technologies. Ceux-ci se voient forcés d'apporter leur collaboration aux enquêtes antiterroristes des autorités chinoises, notamment en fournissant un moyen de déchiffrer les communications établies via leurs technologies.

Cette nouvelle législation, qui s'applique à toutes les entreprises présentes dans l'Empire du Milieu, risque de créer des tensions avec des fournisseurs comme Apple ou Samsung. Après le scandale des écoutes de la NSA américaine, révélées par Edward Snowden, ces entreprises ont proposé à leurs utilisateurs des technologies de chiffrement de bout en bout, dans lesquelles ce sont les utilisateurs eux-mêmes qui sont en possession des clefs. Apple explique ainsi ne pas être en mesure des déchiffrer les communications de iOS, son système d'exploitation mobile, même en cas de requête officielle des services de police. Ces choix d'architecture, qu'on retrouve également au sein de nombre de messageries instantanées, sont au centre de nombreux débats, en France mais surtout aux Etats-Unis, où les candidats à l'élection présidentielle se sont tous prononcés pour l'existence d'un moyen technique d'accès aux données chiffrées.

Pas de backdoors dans la loi, des backdoors dans les faits

Admettant que plusieurs pays et entreprises ont exprimé leurs inquiétudes sur les conséquences de ce projet de loi, Li Shouwei, vice-président de la commission parlementaire en charge des questions technologiques, assure dans un communiqué que la Chine a tenu compte des « *leçons apprises d'autres pays* » et que la législation est similaire aux pratiques d'autres nations dans le monde. En réalité, la loi chinoise devance des projets qui sont en train de poindre dans les grandes démocraties occidentales. Un projet de loi en ce sens est ainsi en cours d'examen en Grande-Bretagne.

Par ailleurs, Li Shouwei assure que la nouvelle réglementation « *n'affectera le fonctionnement normal des entreprises et n'imposera pas l'installation de backdoors afin de violer la propriété intellectuelle des entreprises, la liberté d'expression des citoyens ou leur liberté de culte* ». Toutefois, dans les faits, requérir l'interception de communications chiffrées de bout en bout avec des technologies dont les clefs sont entre les seules mains des utilisateurs revient à imposer aux fournisseurs d'installer des portes dérobées.

Les experts en sécurité estiment qu'introduire une faille de sécurité ne fait que dégrader la sécurité globale d'un système, la vulnérabilité pouvant être réexploitée par d'autres, à des fins malveillantes. La récente affaire Juniper a permis de mesurer combien ce scénario est tout à fait réaliste.

Une menace qui pèse lourd

La législation de Pékin risque également de mettre les fournisseurs en porte-à-faux avec les associations de défense des droits de l'homme. Le gouvernement chinois étant régulièrement accusé d'instrumentaliser les lois antiterroristes pour réprimer les mouvements séparatistes ouïghours, minorité musulmane turcophone du Xinjiang. Il y a quelques jours, Pékin a expulsé la journaliste française Ursula Gauthier, la correspondante de l'Obs accusée par les autorités de minimiser la réalité du terrorisme ouïghour.

La loi que vient de voter l'Assemblée nationale populaire chinoise prévoit encore de mettre à contribution les opérateurs et FAI afin de repérer et bloquer les contenus terroristes ou extrémistes. Ces entreprises sont aussi priées de diffuser des discours luttant contre l'endoctrinement par les groupes terroristes. Faute de ses plier à ces contraintes, les entreprises sont menacées de voir leurs activités interdites en Chine, un marché de 700 millions d'internautes.

A lire aussi :

Juniper : une backdoor made in NSA… récupérée par une organisation inconnue

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

©-Karen-Roach-Shutterstock