Chiffrement : la CNIL casse les backdoors

A l'occasion de la présentation de son rapport annuel, la CNIL (Commission Nationale Informatique et Liberté) s'est invitée dans le débat sur le chiffrement et plus encore sur celui des backdoors. Un sujet d'actualité dans le monde avec l'affaire qui a opposé le FBI à Apple, mais aussi en France sur les affaires de terrorisme. Le procureur de Paris, François Molins a souligné à l'AFP que « *tous les smartphones qu'on essaie d'exploiter sont verrouillés et cryptés. C'est un gros souci car si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans le téléphone. On a toujours un téléphone dans l'affaire Ghlam (mis en examen pour un attentat avorté à Villejuif) dans lequel on n'a pas pu pénétrer. L'an dernier on a eu 8 smartphones qui n'ont pas pu être pénétrés.* »

Un arsenal déjà bien fourni

La demande des autorités judiciaires est donc de pouvoir accéder à ces terminaux soit par des backdoors mises en place par les constructeurs ou par des clés maîtres capables de déchiffrer le contenu des terminaux. La CNIL considère sur ce point qu'il existe « *déjà une réglementation relative aux moyens de cryptologie et un cadre légal bien établi concernant différents types d'accès aux données informatiques dans le cadre de procédure judiciaire* ». Et de lister un ensemble d'outils disponibles : « *Réquisitions numériques, accès aux données de connexions, interception des correspondances, enregistrements audio-visuels, captation des données informatiques affichées à l'écran ou introduites au clavier (keylogger), ou encore le recours à des experts techniques dans le cas de données chiffrées.* »

A cela s'ajoute, *« le droit pénal qui contient des incitations concernant la remise des clés de chiffrement »* des personnes mises en causes. Une obligation néanmoins peu contraignante dans les faits, constate la Commission. Un listing à la Prévert qui sonne comme un tacle au Gouvernement qui a légiféré à plusieurs reprises pour renforcer l'arsenal judiciaire et des services de renseignement.

Les backdoor, une mauvaise solution

Fort de cet arsenal de solutions, la mise en place de backdoors ou de clés maîtres « *ne sont pas la bonne solution* », constate la CNIL. Les arguments sont connus et ont été développés dans l'affaire Apple *versus* FBI. La mise en place d'une porte dérobée dans un logiciel le fragilise en abaissant le niveau de sécurité. Laissant pour le coup la porte ouverte à des opérations de cybercriminalité ou des attaques provenant des Etats. La mise en œuvre de ses solutions est complexe et coûteuse. En conséquence, ces solutions fragiliseraient l'avenir de l'écosystème du numérique.

La CNIL réitère sa confiance dans le chiffrement comme contribuant « *à la résilience de nos sociétés numériques et notre patrimoine informationnel* ». Le débat est donc relancé par la CNIL à un moment où les parlementaires étaient récemment montés au créneau pour menacer les constructeurs de smartphones d'amendes pour refus de collaboration dans les affaires de terrorisme.

A lire aussi :

Protection des données : la Cnil tape sur les doigts de Numericable

Loi Lemaire : la CNIL va-t-elle pouvoir montrer les crocs ?

Crédit photo : Jne Valokuvaus-Shutterstock