WiFi interdit, Tor bloqué, backdoors : les services de police en roue libre

Un document obtenu par Le Monde ce week-end fait état des nouvelles demandes des services de police et de gendarmerie pour, officiellement, mieux lutter contre la menace terroriste. Compilée par la Direction des libertés publiques et des affaires juridiques (DLPAJ), un service dépendant du ministère de l'Intérieur qui prépare deux projets de loi (l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme), cette liste de courses montre que les services de sécurité entendent bien pousser leur avantage, dans un contexte politique où le pouvoir exécutif n'a plus grand chose à leur refuser. Quitte à verser dans le grand n'importe quoi.

Car les mesures envisagées – interdiction du WiFi public, blocage des communications par le système d'anonymisation Tor, obligation d'intégrer des backdoors pour les applications de VoIP comme Skype – ont toutes les chances d'être inefficaces si elles venaient à être votées. D'abord, parce qu'à la lumière des récents attentats (mais également de ceux qui – malheureusement – les ont précédés), la faiblesse des services de renseignement hexagonaux et européens réside davantage dans le traitement et le croisement des données, que dans la collecte de nouvelles informations.

Bannir Tor, Hornet, les proxy, les VPN…

Ensuite, ces blocages ont toutes les chances d'être inefficaces, car très simples à contourner ou impossibles à mettre en œuvre. Au-delà même de sa faisabilité – qui passe par la participation active des FAI -, le blocage de Tor n'aurait un intérêt que s'il s'agissait là de la seule façon d'anonymiser son trafic sur Internet. Mais il y a aussi Hornet, une solution comparable. Ou encore les proxy (ou serveurs mandataires), accessibles via un simple greffon dans le navigateur. Sans oublier les VPN. Comment le législateur compte-t-il s'y prendre pour bannir toutes ces technologies du territoire national ?

Pour les messageries, le constat est peut-être encore plus noir. Déjà, quelle que soit la pression exercée par le gouvernement français, on voit mal les éditeurs de ces solutions céder à une demande d'implantation de backdoor. Tout simplement parce que cela aurait pour conséquence de détourner des millions d'utilisateurs partout dans le monde de leurs services. Ensuite, les messageries instantanées sont si nombreuses qu'on imagine mal les services de sécurité français maîtriser seuls, avec leurs petits bras musclés, un environnement aussi protéiforme. Quant au blocage des quelque 13 millions de points d'accès WiFi que compte l'Hexagone…

En réalité, à moins qu'il ne s'agisse là de fausses pistes, cette nouvelle liste de cadeaux de Noël réclamés par les services de police témoigne d'un fonctionnement en roue libre. Une caricature inquiétante après une première série d'exigences (croisement des données personnelles de l'Etat, émetteurs GPS dans les voitures de location, extension de l'usage des IMSI catchers) qui, si elle représentait déjà un sérieux coup de canif aux libertés individuelles, était suffisamment réaliste et ciblée pour être discutée à peu près sereinement.

A lire aussi :

Chiffrement : comment l'Etat Islamique sécurise ses communications

Après les attentats : faut-il mieux encadrer le chiffrement ?

Crédit photo : David Stuart Productions / Shutterstock