Loi antiterroriste : la France bricole un Patriot Act du pauvre

Nouvelle polémique en vue sur le rôle des intermédiaires techniques. Le projet de loi de lutte contre le terrorisme, dont Le Figaro dévoile aujourd'hui les grandes lignes, prévoit en effet que les fournisseurs d'accès, plates-formes Internet (Google, Facebook, Twitter….) et opérateurs soient soumis à de nouvelles obligations, synonymes d'investissements pour ces acteurs. La première demande de l'Etat vise à les contraindre de « *détecter, par un traitement automatique, une succession suspecte de données de connexion* ». Les sociétés soumises à ce régime devraient ainsi se muer en auxiliaires de police, **détectant proactivement des comportements suspects** en fonction d'instructions qu'elles auront reçues. On ignore pour l'heure si ces comportements suspects se limiteront à la consultation des sites considérés comme faisant l'apologie du terrorisme, ou si l'usage de logiciels particuliers (comme Tor par exemple) suffira à figurer sur la liste noire…

C'est une ordonnance du Premier ministre, donc sans implication d'un juge, qui désignera les opérateurs et sites Internet devant se plier à cette détection de comportements suspects. La mesure apparaît comme la suite logique de la loi de novembre 2014 qui avait retenu « *la consultation habituelle de sites Internet appelant à la commission d'actes de terrorisme* » comme un des éléments constitutifs d'une entreprise de terrorisme individuel.

La seconde obligation qu'évoque le projet de loi risque de faire, elle aussi, couler beaucoup d'encre. Elle prévoit que les autorités disposent des **clefs permettant de lire des conversations interceptées quand celles-ci sont chiffrées**. Les modalités d'application de cet article seront évidemment essentielles et devront être examinées avec soin : comment sera encadré l'accès aux clefs ? ; les autorités auront-elles en main les moyens de déchiffrer toutes les communications émises par une plate-forme (via une backdoor par exemple) ou sera-t-on dans un fonctionnement au cas par cas ? ; dans quels cas cette procédure de déchiffrement sera-t-elle appliquée ? ; quel contrepouvoir contrôlera ces accès ? ; quelle sera sa crédibilité ? Autant de questions essentielles surtout que les données recueillies par les services de renseignement pourront être conservées durant 5 ans, et non plus une seule année, toujours selon *Le Figaro*.

Une collaboration couverte par le secret défense

Si la mesure contre le chiffrement pourra être aisément contournée via des solutions tierces, elle devrait susciter un malaise dans l'industrie, qui utilise la cryptographie pour tenter de regagner la confiance des utilisateurs. Lors de son déplacement aux Etats-Unis le 20 février, où il avait rencontré les dirigeants de Facebook, Apple, Google et Twitter, Bernard Cazeneuve (photo), le ministre de l'Intérieur, avait expliqué que la question du chiffrement était une « *question centrale* » dans les relations des Etats avec les acteurs du Net. Une position proche de celle de David Cameron qui avait clairement pris position contre l'existence de moyens de communication ne permettant pas aux autorités de surveiller ce qui s'écrit ou se dit.

Pour la mise en œuvre de ces mesures, les entreprises concernées devront respecter le secret de la défense nationale, autrement dit ne pas dévoiler leurs échanges avec les autorités françaises en la

matière. Les locaux de ces sociétés pourront être contrôlés par une nouvelle autorité, la Commission nationale de contrôle des techniques de renseignement (CNCTR). Bref, les modalités de la collaboration entre acteurs privés et autorités resteront sécrètes. Exactement comme aux Etats-Unis avec le Patriot Act.

Miser sur le privé ?

Bref la finalité des mesures proposées par le ministre de l'Intérieur, Bernard Cazeneuve, s'apparente à celles qui avaient prévalu dans l'Amérique post-11 septembre : collecte de vastes quantités de métadonnées, capacité à accéder aux informations échangées à posteriori, utilisation de moyens d'écoute spécifiques sur simple autorisation administrative (le projet de loi prévoit l'utilisation de **micros, keyloggers, caméras espions ou balises GPS** mais aussi le **piratage de systèmes tiers**). Principale différence par rapport au dispositif américain tel qu'il apparaît au fil des révélations d'Edward Snowden : là où les Etats-Unis misent largement sur les collectes massives et indifférenciées de données par la NSA (pour ensuite remonter l'histoire de personnes ciblées par les renseignements), la France semble se reposer plutôt sur des sociétés privées qui, par leur nature, engrangent de vastes quantités de données. Une simple façon de compenser la différence de budget entre les services de renseignement américain et français ?

Cette nouvelle loi, présentée jeudi en conseil des ministres, viendra muscler un arsenal déjà considérablement renforcé ces derniers mois. L'article 20 de la Loi de programmation militaire (LPM), dont le décret a été publié le 26 décembre dernier, organise ainsi déjà la collecte de données par les autorités sur les réseaux des hébergeurs, opérateurs télécoms et FAI, en l'**absence de toute réquisition judiciaire**. Mais limite la collecte aux seules métadonnées (identités de l'utilisateur et, le cas échéant, du destinataire, dates et heures des communications…). Une limitation en réalité apparue dans le décret d'application, sur pression de la CNIL, alors que le texte de loi originel avait retenu une formulation très vague (« des informations et documents »). La loi anti-terroriste que prépare actuellement le gouvernement viendra donc étendre les obligations des sociétés privées, sans, semble-t-il, remettre fondamentalement en cause ce canevas excluant la collecte massive de données par les autorités directement sur les réseaux des opérateurs. Mais, via les mesures techniques concernant la pose de mouchards – couplées au déchiffrement -, les renseignements français s'ouvrent **un accès au contenu des communications de leurs cibles**. Toujours sans réquisition judiciaire.

5 sites bloqués

La volonté du gouvernement de bloquer les contenus faisant l'apologie du terrorisme sur Internet a, là encore, déjà donné naissance à des dispositions législatives transcrites dans le droit français. Une précédente loi de lutte contre le terrorisme, votée en novembre dernier et dont le décret d'application a été publié début février, misait ainsi sur la collaboration des intermédiaires techniques. Ce texte prévoit que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), un service de la police nationale, dresse la liste des sites à suspendre, réclame leur retrait à leur hébergeur ou éditeur et en avertit les fournisseurs d'accès afin d'assurer la redirection des requêtes vers une page d'avertissement (voir la capture ci-dessus). Hasard du calendrier, 5 sites sont ainsi bloqués depuis le 15 mars.

Lors du Forum International de la Cybersécurité, qui se tenait à Lille en janvier, Bernard Cazeneuve avait dépeint la lutte contre le prosélytisme en ligne comme une « *co-production* » entre public et privé.

A lire aussi :

Après les attentats : l'Intérieur bricole un plan d'action, pas un Patriot Act
Loi anti-terroriste : un arsenal tout juste renforcé et bientôt chamboulé ?
Accès administratifs aux données de connexion : pareil qu'aujourd'hui… mais en pire