Loi anti-terroriste : un arsenal tout juste renforcé et bientôt chamboulé ?

Même pas encore sec et déjà remis en cause. Le dispositif français de lutte contre le terrorisme est en train d'être considérablement renforcé via, d'un côté, la **Loi de programmation militaire** (en particulier son article 20) et, de l'autre, via **la loi contre le terrorisme** votée en novembre dernier et incluant des mesures de blocage administratif des sites Internet (le projet de décret vient tout juste d'être transmis à Bruxelles comme l'a révélé NextInpact). Le hasard du calendrier a voulu que cet arsenal soit en passe d'entrer en vigueur au moment même où la France est visée par une série d'attentats meurtriers, qui ont causé une vive émotion dans le pays.

Un contexte qui, évidemment, pousse certains politiques à se lancer dans la surenchère. D'où **l'évocation d'un Patriot Act à la française**. Les deux sujets déjà visés par les textes de loi parus en fin d'année dernière – prosélytisme sur Internet ou sur les réseaux sociaux et amélioration du système des écoutes – figurent ainsi parmi le catalogue de mesures évoquées par Manuel Valls et le gouvernement pour renforcer la lutte contre le terrorisme après les attentats de début janvier. Ce matin, sur France Inter, l'ex-Premier ministre François Fillon évoquait la possibilité d'intercepter non plus seulement les métadonnées des échanges électroniques dans le cadre d'écoutes administratives mais également les contenus.

Plus que les seules métadonnées ?

Rappelons que l'article 20 de la Loi de programmation militaire (LPM) organise la collecte de données par les autorités sur les réseaux des hébergeurs, opérateurs télécoms et FAI, en l'**absence de toute réquisition judiciaire**. Mais **ne prévoit pas la pose de mouchards** exploités directement par les services de renseignement sur les réseaux de ces opérateurs (contrairement aux pratiques de la NSA donc) et **limite la collecte aux seules métadonnées** (identités de l'utilisateur et, le cas échéant, du destinataire, dates et heures des communications…). Une limitation 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 »).

Sur le terrain du blocage administratif des services électroniques, dispositif intégré à la loi du 13 novembre dernier, le dispositif – dont on attend le décret d'application donc – prévoit que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) puisse réclamer à un éditeur online ou à un hébergeur le **retrait d'un site**. A défaut, les FAI peuvent aussi être mobilisés par ces requêtes. Les acteurs sollicités devront répondre sous 24 heures. La loi de novembre dernier prévoit également le **déréférencement des sites** faisant l'apologie du terrorisme sur les moteurs de recherche.

« *Plus que des lois, des moyens* »

C'est cet arsenal tout neuf que le gouvernement s'apprête – selon toute vraisemblance – à retoucher. Une volonté qui ne fait pas l'unanimité. Ce matin, tout en soulignant la solidarité du

secteur avec Charlie Hebdo, **Guy Mamou-Mani**, le président de Syntec Numérique, a expliqué, lors de la cérémonie des vœux de la chambre patronale des SSII et éditeurs, qu'il serait « *excessif de rechercher des solutions immédiates inspirées du modèle américain post 11 septembre* », mettant en garde contre des « *procédures d'exception* ». De son côté, le général d'armée **Marc Watin-Augouard**, un des organisateurs du FIC (Forum International de la Cybersécurité, qui se tient la semaine prochaine à Lille), évoque davantage la question des moyens. « *Plus qu'un renforcement de l'arsenal législatif, c'est sur la question des moyens humains et matériels mis à disposition des services de renseignement et d'enquête qu'il faut se concentrer*, explique-t-il dans un entretien avec la rédaction. *Par exemple pour pratiquer à grande échelle de la géolocalisation en temps réel, autorisée à titre préventif par la LPM. Le droit français possède un élément fort avec le délit d'association de malfaiteurs permettant de démanteler des filières. Mais, pour mettre en évidence ce délit, il faut des capacités d'investigation appropriées.* »

A lire aussi :

Accès administratifs aux données de connexion : pareil qu'aujourd'hui… mais en pire

Loi de programmation militaire : l'article 13, juste la partie émergée de l'iceberg ?

Programmation militaire : le Parlement adopte l'extension de la surveillance électronique

Crédit photo : spiber.de / Shutterstock