Non, la France ne vient pas d'adopter un Patriot Act

ANALYSE

Par Laurent Borredon
Service France

Le Parlement français a-t-il voté, mardi 10 décembre, un Patriot Act, du nom de la loi d'exception votée aux Etats-Unis au lendemain des attentats du 11 septembre 2001 ? Le lobby des géants de l'Internet, par la voix de l'Association des services Internet communautaires – ASIC, qui rassemble entre autres AOL, Facebook, Yahoo!, etc. –, a bruyamment alerté l'opinion sur ce thème. Il a été suivi par plusieurs défenseurs des libertés publiques et du respect de la vie privée sur Internet. Une alliance contre nature entre ces derniers et les entreprises qui ont fait de l'utilisation de nos données personnelles à des fins mercantiles leur modèle de croissance a ainsi vu le jour.

Las, la loi de programmation militaire adoptée définitivement par le Sénat, mardi, s'efforce au contraire de clarifier et d'adapter notre droit à des évolutions technologiques qu'on pouvait à peine soupçonner lorsque la loi de 1991 sur les interceptions de sécurité (les écoutes par les services de renseignement, aussi appelées écoutes administratives) a été adoptée. De manière imparfaite, certes, mais sans justifier un tel tollé.

Au départ, le texte rédigé par le gouvernement prévoit de *« légaliser »* l'usage de la géolocalisation en temps réel par les services de renseignement. Non pas que cet usage ait été illégal jusque-là, mais les textes de lois applicables à l'accès aux données de connexion (informatiques et téléphoniques) ne le prévoyaient pas explicitement. Un vide juridique dans lequel opérateurs et services pouvaient aisément s'engouffrer.

Les parlementaires, dont l'intérêt renouvelé pour la question du contrôle des services de renseignement est un signe positif, ont mené un travail de fond. Le président de la commission des lois du Sénat, Jean-Pierre Sueur (PS, Loiret), a estimé que le dispositif gouvernemental sur la géolocalisation en temps réel présentait un défaut : le projet prévoyait de l'intégrer au dispositif d'autorisation issu de la loi antiterroriste de 2006. Une loi dérogatoire, provisoire, qui arrive à échéance en 2015.

Car, en France, deux systèmes d'autorisation administrative d'accès aux données de connexion coexistaient jusque-là. Dans un rapport publié en mai, le président de la commission des lois de l'Assemblée nationale, Jean-Jacques Urvoas (PS, Finistère), avait dénoncé l'*« inutile complexité »* liée à cette cohabitation. Un premier système est lié à la loi de 1991. Pour préparer une écoute téléphonique, les agents de services peuvent demander les données de connexion de leur cible. La demande passe par la Commission nationale de contrôle des interceptions de sécurité (CNCIS), une autorité indépendante. Elle ne concerne que les motifs prévus par la loi de 1991 : sécurité nationale, sauvegarde des éléments essentiels du potentiel scientifique et économique, prévention du terrorisme, de la criminalité et de la délinquance organisées, et reconstitution ou maintien de groupements dissous.

Rideau de fumée

Un second système, voté en 2006 et réservé à la lutte antiterroriste, permet aux services de se procurer auprès des opérateurs des données figurant sur les factures détaillées (identité des personnes entrées en communication, date et durée de l'échange), de localiser un téléphone portable ou un ordinateur, et de connaître les données de connexion Internet (numéro de protocole, date et durée). Une personnalité qualifiée, nommée par la CNCIS, assure un contrôle de légalité a priori des demandes, et la CNCIS contrôle a posteriori.

Les sénateurs, sous l'impulsion de M. Sueur et avec l'accord du gouvernement, ont donc décidé d'unifier les deux systèmes, en intégrant explicitement le « temps réel ». Le contrôle choisi est celui de la personnalité qualifiée sous le contrôle de la CNCIS – limité, certes, car elle ne compte que cinq membres.

Faire la liste des erreurs commises par le lobby des géants du Web dans cette affaire serait fastidieux. Deux sortent du lot. En affirmant que la loi *« supprime le contrôle par un magistrat de l'accès aux données »*, l'ASIC mélange les interceptions de sécurité, qui n'ont jamais fait l'objet du contrôle d'un juge, et les interceptions dans le cadre d'enquêtes judiciaires. Quand l'ASIC s'inquiète de la possibilité offerte aux services d'accéder à ces données en court-circuitant les opérateurs parce que la loi évoque la *« sollicitation du réseau »* par les agents, elle oublie la fin de la phrase : *« transmis en temps réel par les opérateurs »*.

Que cache le rideau de fumée répandu par les opérateurs de l'Internet ? La réalité des échanges entre ces derniers et les services, qui dépassent largement les demandes précises et motivées qui sont couvertes par le cadre légal dont on discute ici. L'article de loi concerne ce qu'on pourrait appeler du « small data », par opposition au « big data », un accès massif et indéterminé à nos données personnelles, dont l'Agence nationale de sécurité américaine (NSA) se nourrit quotidiennement, et dans lequel, selon les éléments réunis par *Le Monde*, la Direction générale de la sécurité extérieure ne se prive pas de piocher non plus. La réalité d'une surveillance qui se branche désormais directement sur les câbles de télécommunication.

Si l'on peut reprocher quelque chose aux parlementaires, c'est d'avoir réglementé la partie émergée d'un iceberg dont on commence à peine à mesurer aujourd'hui la profondeur. ■

borredon@lemonde.fr

LA LOI VOTÉE S'EFFORCE DE CLARIFIER ET D'ADAPTER NOTRE DROIT AUX ÉVOLUTIONS TECHNOLOGIQUES