Collecte de données : le renseignement français aimerait s'inspirer de la NSA

L'article 13 du projet de loi de programmation militaire, qui élargit les possibilités de surveillance électronique des services de renseignement hexagonaux, **inquiète les organisations professionnelles**, comme l'Asic (l'Association des services Internet communautaires qui compte dans ses rangs Google, Facebook, Microsoft, Dailymotion ou Deezer), et fait sortir la Cnil de son silence.

En cause : une disposition de ce texte, actuellement débattu à l'Assemblée Nationale, qui permet aux autorités en charge du renseignement et de la lutte contre la délinquance au sens large (ministère de la Défense, de l'Intérieur, de l'Economie et des Finances) et à leurs agences (Tracfin dans le cadre de la lutte contre les circuits financiers clandestins, rattachée à Bercy) de **disposer d'un « *accès administratif* »** (c'est-à-dire hors décision judiciaire) aux données des internautes que les FAI et hébergeurs conservent au nom de la loi. Et cet accès serait **en « *temps réel* » par « *sollicitation du réseau* »**. L'Asic redoute donc que ce texte n'ouvre la voie à l'installation de dispositifs d'interception directement sur les équipements de hébergeurs, fournisseurs d'accès ou de services et opérateurs. **L'équivalent du programme Prism de la NSA donc**.

Récolter les métadonnées

Cette disposition ne signifie pas un accès aux contenus des messages transmis par téléphone ou par Internet, mais le champ des données concernées est vaste : détails des factures télécoms (liste des numéros appelés et appelant, durée et date des communications), « données techniques relatives à l'identification des numéros d'abonnement » et « localisation des équipements terminaux utilisés ». Bref, l'équivalent des méta-données recueillies par les services de renseignement américains dans le cadre de leurs nombreux programmes d'écoutes.

L'Asic demande au gouvernement d'instaurer un **moratoire sur tout nouveau texte destiné à créer un régime d'exception** en matière d'accès aux données des utilisateurs Internet. Un moratoire qui doit servir à établir un audit complet des dispositifs créés par la loi et mis en œuvre par les divers services, s'assurer de l'existence de garde-fous suffisants et une analyse chiffrée du nombre de réquisitions adressées par les autorités aux divers acteurs de l'Internet.

La Cnil ? Bien peu de poids dans le débat

Dans un communiqué, la **Cnil** indique de son côté qu'elle n'a **pas été saisie de ce fameux article 13 du projet de loi. Et** précise des circonstances dans lesquelles la réquisition de données de connexion dans un cadre d'enquête administrative pourra être effectuée : « recherche de renseignements au nom de la sécurité nationale », « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ». Bref un spectre très large. En tout cas bien plus large que le régime d'exception existant pour les affaires

de lutte antiterrorisme (loi anti-terrorisme de 2006).

On l'a compris : concernant l'extension des régimes d'exception relatifs à la surveillance électronique (au-delà de la lutte anti-terrorisme), la CNIL n'a pas vraiment eu de droit de regard.

Sur d'autres volets du projet de loi, elle a juste été auditionnée par les Commissions des lois et de la Défense du Sénat (à défaut d'avoir été consulté). C'est le cas de l'accès aux données de connexion en temps réel, et, par voie de conséquence, de la **géolocalisation des terminaux mobiles** (smartphones, etc.) des personnes en temps réel.

Sur ce dernier point, le Sénat a **modifié le régime juridique de la géolocalisation** en lui appliquant **celui des interceptions de sécurité**. « *Cette modification a été adoptée en Commission par l'Assemblée nationale à l'occasion de l'examen du texte en première lecture* », indique la Cnil.

Une évolution à rapprocher avec deux arrêts récents de la chambre criminelle de la Cour de cassation (22 octobre) : la géolocalisation en temps réel des personnes soupçonnées de délits ou de crimes grâce à leurs téléphones portables ne pourra plus avoir lieu dans le cadre d'une enquête préliminaire, selon Le Figaro. L'aval d'un juge sera donc nécessaire.

Rappelons que, fin octobre, **la Cnil a saisi le gouvernement d'une demande de précisions** sur l'éventuelle existence d'un programme français similaire au programme américain de cybersurveillance Prism, « qui serait ainsi réalisé en dehors du cadre juridique prévu par le législateur ». On attend toujours la réponse de l'exécutif.

Credit photo : Shutterstock.com – Copyright : Andrey_Popov

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes