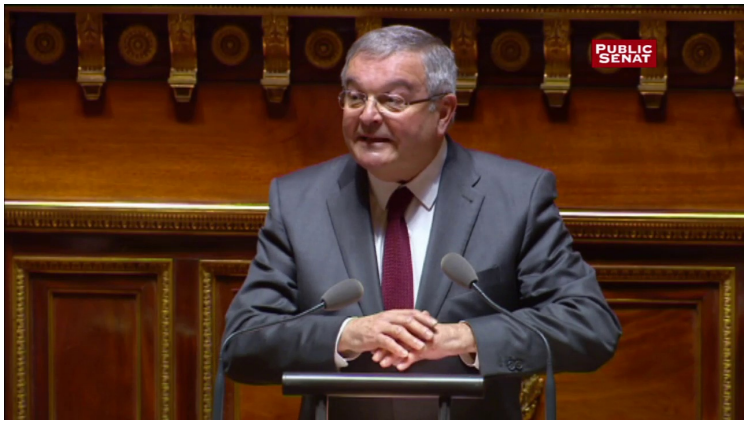
Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama