ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 84388	De **M. Éric Ciotti** (Les Républicains - Alpes-Maritimes)	**Question écrite**
Ministère interrogé > Justice	**Ministère attributaire** > Justice	
Rubrique >ordre public	**Tête d'analyse** >terrorisme	**Analyse** > filières djihadistes. surveillance. commission d'enquête. rapport.
Question publiée au JO le : **07/07/2015** Réponse publiée au JO le : **19/04/2016** page : **3446** Date de changement d'attribution : **28/01/2016**		

Texte de la question

M. Éric Ciotti attire l'attention de Mme la garde des sceaux, ministre de la justice sur la proposition du rapport de la commission d'enquête sur la surveillance des filières et des individus djihadistes visant à créer un régime de saisie des données informatiques à l'insu de leurs propriétaires et donc indépendant du régime de la perquisition. Il lui demande son avis sur cette proposition.

Texte de la réponse

Dans le domaine de la lutte contre le terrorisme l'enjeu de l'utilisation de techniques spéciales d'enquête permettant de capter des données informatiques est devenu fondamental, tant il est constant que les moyens classiques de communication, notamment téléphoniques, ont été largement délaissés au profit de l'internet. Si les interceptions de communications et captations de données privées demeurent des procédures exceptionnelles, et parce qu'elles permettent de déroger au principe du secret des correspondances, elles doivent se faire dans un cadre juridique parfaitement établi. L'atteinte à la vie privée susceptible de découler de la mise en œuvre de ce type de techniques d'enquête justifie qu'elles soient subordonnées à de strictes garanties procédurales. Ainsi, le régime des perquisitions à distance, nécessitant par principe une publicité de la mesure à l'égard du perquisitionné, son consentement ou à tout le moins sa présence, ne permet pas de saisir des données à distance sans en informer le suspect. L'article 57-1 du code de procédure pénale prévoit en effet que les officiers de police judiciaire peuvent au cours d'une perquisition accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Il a été modifié par la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme afin de préciser que les officiers de police judiciaire peuvent, dans les conditions de perquisition prévues au même code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique. Mais la loi précitée n'a pas modifié les garanties dont bénéficie la personne au titre des articles 57 et 76 du code de procédure pénale. Ces dispositions interdisent à l'enquêteur de consulter et saisir des données en dehors de la présence de l'intéressé, d'un tiers désigné ou de deux témoins.La captation de données informatiques prévues par les articles 706-102-1 à 706-102-6 du code de procédure pénale a vocation à répondre à cette problématique en permettant une captation à l'insu de la personne. Du fait de son caractère fortement intrusif et afin de ne pas éluder les garanties fondamentales apportées par le système judiciaire, cette technique spéciale d'enquête peut uniquement être mise en œuvre pour les enquêtes relatives aux faits les plus graves, entrant dans le champ de la criminalité

organisée ou du terrorisme. L'article 706-102-1 du code de procédure pénale définit la captation de données comme la mise en place « d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les a introduit par la saisie de caractères ». Ce dispositif permet aux enquêteurs de prendre connaissance en temps réel de tous types de fichiers, qu'ils soient émis par voie de télécommunications ou stockés sur un support physique. Il a pour effet de mettre l'enquêteur dans la situation de quelqu'un qui observerait derrière lui l'utilisateur d'un ordinateur. La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a en outre étendu le dispositif permettant de capter des données informatiques à l'insu de la personne en prévoyant la possibilité de capter les données reçues ou émises par des périphériques audiovisuels, afin de prendre en compte l'utilisation de logiciels de téléphonie par ordinateur, du type de Skype, par exemple. Enfin, il convient de préciser que cette technique ne se heurte pas au problème du chiffrement.