

14ème législature

Question N° : 88951	De M. Thierry Lazaro (Les Républicains - Nord)	Question écrite
Ministère interrogé > Justice		Ministère attributaire > Justice
Rubrique >ordre public	Tête d'analyse >terrorisme	Analyse > djihad. lutte et prévention.
Question publiée au JO le : 22/09/2015 Réponse publiée au JO le : 06/12/2016 page : 10148 Date de changement d'attribution : 28/01/2016 Date de renouvellement : 05/01/2016 Date de renouvellement : 10/05/2016 Date de renouvellement : 16/08/2016 Date de renouvellement : 22/11/2016		

Texte de la question

M. Thierry Lazaro attire l'attention de Mme la garde des sceaux, ministre de la justice sur le rapport parlementaire fait au nom de la commission d'enquête sur l'organisation et les moyens de la lutte contre les réseaux djihadistes en France et en Europe. Ce rapport relève qu'à la date du 9 mars 2015, les services de renseignement avaient recensé un total de 1 432 ressortissants français partis vers les zones de combat syro-irakiennes. Si un tel phénomène n'est pas sans précédent dans notre pays, de tels départs vers des zones de combats ayant déjà eu lieu par le passé, notamment vers la Bosnie, l'Afghanistan, la Somalie ou encore le Mali, son ampleur est, en revanche, inédite. Ce rapport formule des propositions destinées à prévenir la radicalisation, à renforcer la coordination et les prérogatives des services antiterroristes, à contrer le « djihad » médiatique, à tarir le financement du terrorisme, à mieux contrôler les frontières de l'Union européenne et à adapter la réponse pénale et carcérale. Aussi, il souhaite connaître son avis sur la proposition visant à étendre la circonstance aggravante prévue pour les attaques contre les systèmes de traitement automatisé de données (STAD) mis en œuvre par l'État à l'ensemble des STAD mis en œuvre par les opérateurs d'importance vitale au moyen d'une modification des articles 323-3 et 323-4-1 du code pénal.

Texte de la réponse

La proposition no 80 du rapport parlementaire précité est « d'étendre la circonstance aggravante prévue pour les attaques contre les systèmes de traitement automatisé de données (STAD) mis en œuvre par l'État à l'ensemble des STAD mis en œuvre par les opérateurs d'importance vitale au moyen d'une modification des articles 323-3 et 323-4-1 du code pénal ». En effet, le rapport parlementaire indique qu'à l'occasion d'une table ronde relative à l'utilisation d'Internet à des fins d'organisation par les groupes terroristes, Marc Robert, auteur d'un rapport de référence sur la Cybercriminalité en 2014, a rappelé le nombre croissant de cyber-attaques à l'encontre de cibles de l'administration française voire à l'encontre d'entreprises privées. Le droit positif réprime d'abord les atteintes aux STAD mis en œuvre par les opérateurs d'importance vitale par les dispositions générales des atteintes aux STAD (art. 323-1 et suivants CP). Le fait d'accéder, de se maintenir frauduleusement dans un STAD est puni de 2 ans d'emprisonnement et de 60 000 euros d'amende, et de 3 ans d'emprisonnement et de 100 000 euros d'amende en cas de suppression ou de modification de données contenues dans le STAD (art. 323-1 CP). Le fait d'entraver ou de fausser le fonctionnement d'un STAD est lui puni de 5 ans d'emprisonnement et de 150 000 euros d'amende (art.



323-2 CP). Le fait d'introduire frauduleusement des données dans un STAD, ou d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données contenues dans un STAD est également puni de 5 ans d'emprisonnement et de 150 000 euros d'amende. L'association de malfaiteurs pour toutes ces infractions est également réprimée (art. 323-4 CP). D'autre part, l'atteinte aux STAD mis en œuvre par un opérateur d'importance vitale peut remplir le critère d'un acte terroriste (art. 421-1 CP), par exemple si elle est revendiquée par un groupe terroriste identifié. En conséquence, cette atteinte aux STAD est punie d'une peine de 20 ans de réclusion criminelle et de 350 000 euros d'amende. Enfin, l'atteinte aux STAD mis en œuvre par un opérateur d'importance vitale peut être qualifiée d'infraction contre les intérêts fondamentaux de la nation (art. 411-1 cp), notamment la livraison d'informations à une puissance étrangère, voire le simple recueil des données informatiques (art 411-6 à 411-8 CP), mais également le sabotage d'un STAD (art 411-9 CP). Ainsi, le régime de répression des atteintes aux STAD mis en œuvre par les opérateurs d'importance vitale est complet, d'autant que dans le cas d'une cyber-attaque à caractère terroriste ou relevant de l'espionnage, les régimes spécifiques prévoient de lourdes peines dissuasives.