ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 852	De **M. Fabien Gouttefarde** (La République en Marche - Eure)	**Question écrite**
Ministère interrogé > Armées	**Ministère attributaire** > Armées	
Rubrique >droits fondamentaux	**Tête d'analyse** >Conservation des données de connexion	**Analyse** > Conservation des données de connexion.
Question publiée au JO le : **05/09/2017** Réponse publiée au JO le : **19/12/2017** page : **6538** Date de signalement : **28/11/2017**		

Texte de la question

M. Fabien Gouttefarde attire l'attention de Mme la ministre des armées sur les conséquences de l'arrêt de la Cour de justice de l'Union européenne (CJUE) dans les affaires jointes *C-203/15 Tele2Sverige AB/Post-och telestyrelsen* et *C-698/15 Secretary of State for the Homme Department/Tom Watson e.a* du 21 décembre 2016 et sur les dispositions françaises qui prévoient la conservation des données de trafic et de connexion à des fins de lutte contre le terrorisme. Les deux questions préjudicielles suédoise et britannique portaient sur la conformité aux droits à la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, des législations suédoise et britannique qui prévoient la conservation généralisée, par les fournisseurs de services de communications électroniques, des données de connexion des communications électroniques dans le but d'assurer leur disponibilité dans le cadre d'enquête pénale ou de prévention des infractions terroristes. En réponse à ces questions, la Cour reprend très largement le raisonnement qu'elle avait tenu dans l'arrêt *C-293/12 Digital Rights Ireland* du 8 avril 2014, où elle avait jugé qu'une obligation générale de conservation de données excède les limites de ce qui est strictement nécessaire lorsqu'elle n'est pas accompagnée de garanties strictes. La Cour a jugé qu'une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de données était, en elle-même, contraire au droit de l'Union. Cet arrêt, en interdisant que les législations nationales prévoient des conservations généralisées et indifférenciée des données relatives au trafic et aux données de localisation et en rappelant que les mesures envisagées doivent être appropriées, rigoureusement proportionnées et nécessaires, apparaît considérablement restrictif pour plusieurs mesures nationales. Plusieurs techniques de renseignement permettent aux services spécialisés de renseignement relevant du ministère de la défense d'avoir accès aux données de connexion associées aux correspondances électroniques telles que notamment celles des articles du code de la sécurité intérieure L. 851-2 (accès en temps réel à l'exhaustivité des données de connexion associées à des personnes présentant un enjeu en matière de terrorisme), L. 851-3 et L. 851-4 (accès administratifs aux données de connexion). L'idée d'une collecte sélective des données semble peu opérationnelle et impliquerait de faire renoncer les services à l'exploitation administrative ou judiciaire des données de connexion qui repose nécessairement sur une collecte générale et préalable de ces données par les opérateurs dans des objectifs commerciaux. Dans un contexte de menace terroriste élevée, les conséquences d'une telle décision paraissent problématiques au regard de la nécessaire mission de protection des citoyens. Suite à cette décision, certains États membres tels que les Pays-Bas et la Belgique ont fait le choix d'annuler ou de remettre en cause leurs législations en matière de conservation des données. Dès lors, il souhaiterait connaître quelle est la position du ministère de la défense sur cette question et savoir si la loi sur le renseignement du 24 juillet 2015 qui permet l'accès aux données conservées ou transmises par les opérateurs comporte les garanties nécessaires au regard des critères récemment fixées par la CJUE.

ASSEMBLÉE NATIONALE

Texte de la réponse

Dans les affaires Tele2 Sverige et Watson, la Cour de justice de l'Union européenne (CJUE) était appelée à se prononcer sur la conformité au droit de l'Union européenne (directive 2002/58/CE et articles 7, 8, 11 et 52 paragraphe 1 de la Charte des droits fondamentaux) de législations nationales imposant une obligation générale de conservation de données par les opérateurs de services de communications électroniques, sans qu'aucune différenciation, limitation ni exception ne soit prévue, aux fins de lutter contre la criminalité. La CJUE était aussi interrogée sur l'encadrement de l'accès des autorités nationales à ces données, sur les exigences liées à leur protection et à leur sécurité, ainsi que sur leur durée de conservation. Dans son arrêt rendu en grande chambre, le 21 décembre 2016, la CJUE a considéré que relèvent du champ d'application du droit de l'UE des mesures législatives qui imposent aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation ou qui autorisent l'accès des autorités nationales aux données conservées par ces entreprises. Elle s'est ensuite prononcée sur des législations nationales organisant cette conservation aux seules fins de lutte contre la criminalité. Toutefois, la CJUE n'a pas été appelée à se prononcer sur des législations organisant le recueil par les autorités publiques des données de connexion conservées par les fournisseurs de communications électroniques à des fins de police administrative, de défense et de sécurité nationale. Dès lors, cet arrêt n'est pas transposable à la loi no 2015-912 du 24 juillet 2015 relative au renseignement, codifiée au livre VIII du code de la sécurité intérieure, qui poursuit de telles finalités. En tout état de cause, cette loi, qui ne met par elle-même aucune obligation de conservation des données de connexion à la charge des fournisseurs de communications électroniques, comporte les garanties nécessaires quant à l'accès à ces données au regard des critères fixés par la Cour.