ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 72239	De **M. Lionel Tardy** (Union pour un Mouvement Populaire - Haute-Savoie)	**Question écrite**

Ministère interrogé > Défense	**Ministère attributaire** > Premier ministre

Rubrique >défense	**Tête d'analyse** >télécommunications	**Analyse** > loi de programmation militaire 2014-2019. droit communautaire. compatibilité.

Question publiée au JO le : **06/01/2015**
Réponse publiée au JO le : **16/08/2016** page : **7307**
Date de changement d'attribution : **24/02/2015**
Date de renouvellement : **14/04/2015**
Date de renouvellement : **21/07/2015**
Date de renouvellement : **27/10/2015**
Date de renouvellement : **02/02/2016**
Date de renouvellement : **10/05/2016**

Texte de la question

M. Lionel Tardy interroge M. le ministre de la défense sur le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion, pris en application de l'article 20 de la loi de programmation militaire. Dans sa délibération n° 2014-484 du 4 décembre portant avis sur le décret précité, la CNIL relève que l'invalidation de la directive n° 2006/24/CE par la Cour de justice de l'Union européenne dans un arrêt en date du 8 avril 2014 (arrêt « digital rights Ireland ») est intervenue depuis la publication de la loi, et que cette invalidation conduit à s'interroger sur le risque d'inconventionalité des dispositions de la loi de programmation militaire concernées. Il souhaite connaître son analyse à ce sujet.

Texte de la réponse

L'adoption de la loi no 2015-912 du 24 juillet 2015 relative au renseignement a fait évoluer la législation nationale. Les dispositions du décret no 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion ont été remplacées par celles du décret no 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement pris en application de la loi no 2015 912 du 24 juillet 2015 relative au renseignement. Ces nouvelles dispositions règlementaires vont très au-delà des exigences de la Cour de justice de l'Union européenne. Comme il est rappelé dans la question, la Cour de justice de l'Union européenne a invalidé la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 en se fondant sur un ensemble de critères. Outre le fait que la directive couvrait « de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées », la Cour a relevé que la directive ne prévoyait « aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données », ni de « critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure ». La Cour a également constaté que « l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire ». Enfin la Cour a critiqué la durée maximale de conservation des données de vingt-quatre mois et l'absence de règles garantissant la protection et la

sécurité des données. Or le droit national, tant celui antérieur issu de la loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et du décret no 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion que celui actuellement en vigueur issu de la loi no 2015-912 du 24 juillet 2015 relative au renseignement et du décret no 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, définit précisément (article R. 851-5 du code de la sécurité intérieure) les données de connexion que les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet doivent conserver (il s'agit, à l'exclusion du contenu des correspondances échangées ou des informations consultées, des documents énumérés aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret no 2011-219 du 25 février 2011 modifié relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne), ainsi que celles qui peuvent être transmises en temps réel (L. 851-2) ou utilisées par des traitements automatisés (L. 851-3) : les données techniques permettant de localiser les équipements terminaux, relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne, relatives à l'acheminement des communications électroniques par les réseaux, relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne, relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels. En sus, l'article L. 811-3 du code de la sécurité intérieure ne permet l'accès que pour des finalités limitativement énumérées. Par ailleurs, l'article R. 821-1 du code restreint l'accès aux données de connexion à des agents individuellement désignés et spécialement habilités, au sein des services de l'État chargés des missions évoquées ci-dessus. Ces services sont limitativement énumérés à l'article R. 851-1 et R. 851-1-1 du code et seul le ministre ou le directeur dont relèvent les agents peuvent habiliter ces derniers à présenter des demandes d'accès (article R. 821-1). Enfin, le législateur a prévu, à l'article L. 821-1 du code, que la mise en œuvre sur le territoire national des techniques de recueil de ces données est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante qui dispose notamment (article R. 851-10) d'un accès permanent, complet, direct et immédiat aux traitements automatisés correspondants. Ce dispositif a des points communs avec celui en vigueur avant la loi relative au renseignement et selon lequel (article L. 246-2 désormais abrogé) une personnalité qualifiée nommée par une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), avait compétence pour autoriser le recueil des données de connexion après avoir vérifié l'identité des agents, la nature des données demandées et les finalités invoquées, comme le prévoyait l'article R. 246-4 du code. La CNCIS pouvait ensuite, selon l'article L. 246-4 du code, vérifier que les données de connexion avaient été recueillies conformément à la loi et adresser, le cas échéant, des recommandations au Premier ministre, qui était tenu de lui faire connaître les mesures prises en réponse. Pour effectuer son contrôle, la CNCIS pouvait, en application de l'article R. 246-8 du code, accéder à tout moment aux traitements mis en œuvre de manière centralisée et sécurisée par le Premier ministre. Ces traitements, institués aux articles R. 246-5 et R. 246-6 du code, permettaient de suivre l'ensemble du processus puisqu'ils contenaient les demandes des agents, les décisions de la personnalité qualifiée et, en cas de décision positive, les données de connexion recueillies. Il s'avère donc que le dispositif national d'accès administratif aux données de connexion, issu de la loi no 2013-1168 du 18 décembre 2013 et du décret no 2014-1576 du 24 décembre 2014, présentait des garanties telles que le cadre juridique n'aurait su être assimilé à celui censuré par la Cour dans son arrêt du 8 avril 2014. Le décret no 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion n'était donc pas contraire aux stipulations de la Charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la Cour dans son arrêt, comme l'a d'ailleurs jugé le Conseil d'Etat par sa décision no 388134 en date du 12 février dernier. Il en va de même pour le dispositif issu de la loi no 2015-912 du 24 juillet 2015 relative au renseignement et du décret no 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.