

## 15ème législature

<b>Question N° :</b> <b>7361</b>	De <b>Mme Laure de La Raudière</b> ( UDI, Agir et Indépendants - Eure-et-Loir )	<b>Question écrite</b>
<b>Ministère interrogé</b> > Justice		<b>Ministère attributaire</b> > Justice
<b>Rubrique</b> > télécommunications	<b>Tête d'analyse</b> > Métadonnées	<b>Analyse</b> > Métadonnées.
Question publiée au JO le : <b>10/04/2018</b> Réponse publiée au JO le : <b>21/05/2019</b> page : <b>4795</b>		

### Texte de la question

Mme Laure de La Raudière attire l'attention de Mme la garde des sceaux, ministre de la justice, sur la portée de l'arrêt Tele2 rendu le 21 décembre 2016 par la Cour de justice de l'Union européenne qui a ainsi estimé que « les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications électroniques ». Cet arrêt s'inscrit dans le prolongement de l'invalidation, par un arrêt de la CJUE en date du 8 avril 2014 (arrêt *DigitalRights*), de la directive 2006/24/CE sur la conservation des données. Dans une réponse formulée le 7 juin 2016, le garde des sceaux de l'époque avait estimé que cet arrêt était sans impact sur les dispositions nationales, notamment l'article L. 34-1 du code des postes et communications électroniques, dans la mesure où ces dernières sont antérieures à la directive invalidée. Or l'arrêt Tele2 vient infirmer une telle interprétation. Pour la CJUE, les mesures nationales de conservation des données par les fournisseurs de services de communications électroniques relèvent bien du champ d'application du droit de l'Union. Partant de là, la CJUE, sans rejeter le principe même d'une conservation des données de connexion, vient rappeler quelques conditions intangibles devant être scrupuleusement respectées par les législations nationales. En particulier, elle rappelle que le principe fondamental doit rester celui du respect de la vie privée, et que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. La CJUE précise que l'exception (conservation des données de connexion) ne doit aucunement devenir la règle. Or l'article L. 34-1 précité, s'il pose le principe d'un effacement ou anonymisation des données de connexion, prévoit immédiatement une dérogation permettant la conservation des données de connexion pour une durée d'un an. Le non-respect par les fournisseurs de services de communications électroniques de cette disposition est pénalement sanctionné. En outre, pour la CJUE, seule la lutte contre la criminalité grave est susceptible de justifier l'ingérence résultant d'une réglementation nationale prévoyant la conservation des données relatives au trafic et des données de localisation. Par ailleurs, elle conditionne l'accès aux données conservées au respect de plusieurs exigences. Premièrement, l'accès doit être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, ce qui pose la question de la validité des demandes formulées au titre d'enquêtes diligentées sous l'autorité du parquet d'une part et d'autre part du droit de communication de l'administration pour des données conservées par les fournisseurs de services de communications électroniques, dans la mesure où il n'existe à ce jour aucun contrôle préalable des demandes de l'administration, hormis pour les sujets relevant de l'accès administratif aux données de connexion soumis au contrôle de la CNCTR. Deuxièmement, les personnes dont les données conservées ont été demandées par les autorités doivent être informées par ces dernières, dès lors que cette communication n'est pas susceptible de compromettre les enquêtes menées. Enfin, la conservation des données doit avoir lieu sur le territoire de l'Union, ce qui pose la question de la validité de demandes portant sur des données conservées hors de l'Union par de grands acteurs d'Internet. À la suite de cet arrêt, des États membres tels que les Pays-Bas et la Belgique ont suspendu leur régime de conservation des



données de connexion. L'Espagne de son côté a adressé une question préjudicielle sur le périmètre du critère de « criminalité grave ». Quant au juge britannique, il a récemment invalidé le régime national sur la base de l'arrêt Tele2. De son côté, dans un discours à l'Académie de droit européen de Trèves le 19 octobre 2017, le vice-président du Conseil d'État a reconnu la marge d'appréciation des États en ce qui concerne la possibilité d'ordonner la conservation des données de connexion a été considérablement réduite par cet arrêt. Par conséquent, Madame Laure de La Raudière souhaite donc obtenir des précisions quant à la portée de cet arrêt Tele2 sur les procédures initiées au niveau national visant à solliciter de la part des fournisseurs de services de communications électroniques, la transmission de données sur l'activité de leurs utilisateurs. En particulier, dans la mesure où le non-respect des principes rappelés par la CJUE fait peser un risque sur ces procédures, elle souhaite connaître les moyens qu'il compte mettre en œuvre pour mettre en conformité le droit national français avec les prescriptions formulées par la CJUE.

## Texte de la réponse

Par son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne (CJUE) a dit pour droit que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, "lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique". Toutefois, par deux arrêts en date du 26 juillet 2018, le Conseil d'Etat a sursis à statuer dans deux espèces initiées par la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs, dont l'une vise l'article R. 10-13 du code des postes et des communications électroniques et le décret n° 2011-219 du 25 février 2011, jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée notamment sur les questions suivantes : - L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne ? - L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne ? - Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un Etat d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ? D'autres renvois préjudiciels sont par ailleurs en cours devant la CJUE sur cette même matière, interrogeant la Cour tant sur son interprétation de l'obligation de conservation des données que sur les modalités d'accès qu'elle prescrit pour ces dernières. Le Gouvernement est particulièrement attentif aux questions de droit soulevées par ces décisions mais estime nécessaire de recueillir au préalable les précisions demandées notamment par le Conseil d'Etat à la Cour de



Justice de l'Union européenne avant d'apprécier dans quelle mesure il est nécessaire d'adapter le cadre normatif national aux exigences du droit européen.