Réglementations française et européenne de la collecte, conservation et exploitation des données de connexion

Description

Conseil d'État, 21 avril 2021, n° 393099.

La répression des infractions, les garanties de l'ordre et de la sécurité publique et la lutte contre le terrorisme peuvent-elles justifier que les autorités nationales imposent aux opérateurs des services de communications électroniques de collecter, de conserver et de mettre à la disposition des services de sécurité, en diverses circonstances, les données de connexion des internautes utilisateurs ? Ne risque-t-il pas d'être ainsi porté atteinte au droit au respect de la vie privée et à la protection des données personnelles des intéressés ?

À la suite de la contestation par différentes associations comme French Data Network, La Quadrature du Net, la Fédération des fournisseurs d'accès à internet associatifs et Igwan.net, de diverses dispositions réglementaires françaises, et après que, saisie d'une question préjudicielle, la Cour de justice de l'Union européenne (CJUE) s'est, par un arrêt du 6 octobre 2020 (C-511/18, C-512/18 et C-520/18), prononcée sur les conditions de la conformité notamment du droit français au regard des exigences du droit européen en la matière (*La rem* n°54bis-55, p.15), le Conseil d'État, par un arrêt du 21 avril 2021, a statué sur cette question. Validant, sous conditions, certaines mesures, il en a annulé d'autres.

La compréhension de la façon dont est assurée, à cet égard, la conciliation entre les droits des individus, les obligations des opérateurs et les pouvoirs des autorités publiques, implique qu'il soit brièvement fait mention des dispositions nationales et européennes en cause et de l'appréciation qui en ont été faites par les juridictions saisies.

Dispositions en cause

C'est au regard de leur conformité à différentes dispositions européennes qu'ont été examinées les dispositions françaises. S'agissant du droit français, étaient notamment en cause les dispositions du code des postes et des communications électroniques et d'un décret du 25 février 2011 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 des décrets du 28 septembre 2015, du 11 décembre 2015 et du 29 janvier 2016, pris en application du Code de la sécurité intérieure, relatifs aux pouvoirs des services de renseignement en matière d'accès aux données de connexion des utilisateurs des services de communications électroniques.

Était en cause la conformité de ces dispositions au regard du droit européen et notamment des directives

2000/31/CE, du 8 juin 2000, 2002/21/CE, du 7 mars 2002, et 2002/58/CE, du 12 juillet 2000, permettant que soit imposée aux opérateurs de services de communications électroniques une obligation de collecte et de conservation des données de connexion des utilisateurs, incluant leur localisation, et au regard de la Charte des droits fondamentaux de l'Union européenne et du règlement (UE) n° 2016-679, relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel, dit RGPD.

Appréciation des dispositions

Dans leur saisine du Conseil d'État, les requérants contestaient *« les dispositions réglementaires imposant aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus, de conserver, de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs »*, ainsi que celles *« permettant aux services de renseignement de recueillir et d'opérer des traitements sur ces données »*.

Avant de se prononcer, et pour s'assurer de la conformité du droit français au regard du droit européen, le Conseil d'État a saisi la Cour de justice de l'Union européenne (CJUE) d'une question préjudicielle.

Par arrêt du 6 octobre 2020, la CJUE a considéré que les dispositions de la directive 2002/58/CE du 12 juillet 2002, telle que modifiée par la directive 2009/136/CE du 25 novembre 2009, doivent être interprétées en ce qu'elles s'opposent à des mesures législatives prévoyant, *« à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation »* ; mais qu'en revanche elles ne s'opposent *« pas à des mesures législatives permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale »*, et sous condition d'un moyen de *« contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant »* et que ladite injonction ne puisse *« être émise que pour une période temporellement limitée »* . Il a également été jugé que, dans de telles conditions, peuvent être admises des mesures relatives à *« une conservation ciblée des données relatives au trafic et des données de localisation »*, ainsi qu'une *« conservation généralisée et indifférenciée des adresses IP »*.

Se référant à l'article 88-1 de la Constitution, et tout en posant que *« le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet, en laissant au besoin inappliquée toute disposition contraire »* et de *« retenir, de l'interprétation que la CJUE a donnée des obligations résultant du droit de l'Union, la lecture la plus conforme aux exigences constitutionnelles »* , le Conseil d'État pose que *« dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la CJUE, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige »*.

Il ajoute que, si la portée d'une disposition européenne *« n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'UE, il priverait de garanties effectives l'exigence constitutionnelle dont le défendeur se prévaut »*. Il est relevé qu'il *« est soutenu en défense que les dispositions du droit national contestées au motif qu'elles seraient contraires au droit de l'UE ne sauraient être écartées sans priver de garanties effectives les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme »*, et il est considéré qu'il s'agit là d'*« objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée »*.

De l'appréciation de la CJUE, le Conseil d'État conclut que doivent être annulées les dispositions du décret du 25 février 2011 *« en tant seulement »* qu'elles *« ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale »*.

Quant aux dispositions contestées relatives à la conservation générale et indifférenciée des données de connexion aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public, le Conseil d'État estime que *« le Gouvernement ne pouvait pas imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion »*, autres notamment que celles qui sont *« relatives à l'identité civile »* et *« aux adresses IP »*, aux *« fins de lutte contre la criminalité et de prévention des menaces à l'ordre public, sans méconnaître le droit de l'UE »*. Il ajoute que *« l'application du droit de l'UE, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle invoqués par le Premier ministre »*. Il conclut qu'il convient donc d'écarter les dispositions contestées sur ce point, en ce qu'elles *« poursuivent une finalité autre que la sauvegarde de la sécurité nationale »*.

S'agissant des dispositions des décrets du 28 septembre 2015, du 11 décembre 2015 et du 29 janvier 2016, décrets relatifs aux traitements mis en œuvre par les services de renseignement sur les données de

connexion, dont la conformité au droit de l'UE a été critiquée, l'arrêt retient que, à la date à laquelle ces différents décrets *« ont été adoptés, la France était confrontée à une menace grave, réelle et actuelle pour la sécurité nationale »*, dans des conditions telles que pouvait alors être imposée, à l'époque, aux opérateurs de communications électroniques, *« la conservation généralisée et indifférenciée des données de trafic et de localisation, aux fins de sauvegarde de la sécurité nationale »*. Il est considéré que *« l'accès des services de renseignement aux données de trafic et de localisation conservées par les opérateurs »* était alors possible sans méconnaître les exigences du droit européen, mais que *« l'autorité publique ne peut porter atteinte au respect de la vie privée, dans toutes ses composantes, notamment la protection des données à caractère personnel, que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité »*. Relevant que *« la mise en œuvre de la technique de renseignement* […] *ne donne pas lieu au contrôle préalable par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant, dès lors que la Commission nationale de contrôle des techniques de renseignement n'émet qu'un avis simple ou des recommandations non contraignantes »*, il en est conclu que *« le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignements doit être annulé »*.

Pour autant que les exigences du droit européen en matière de protection de la vie privée et des données personnelles, à l'égard des pratiques de collecte, de conservation et d'exploitation des données de connexion aux services de communications électroniques, ne remettent pas en cause les objectifs de valeur constitutionnelle *« de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme »*, elles s'imposent aux autorités nationales. Toutes mesures contraires doivent être déclarées non conformes et doivent donc être annulées.

Categorie

1. Droit

date créée
24 août 2021
Auteur
emmanuelderieux