AJDA

AJDA 2018 p.2027

Conservation des données de connexion : la CJUE invitée à reconsidérer sa jurisprudence

François-Xavier Bréchot, Magistrat administratif, rapporteur public à la cour administrative d'appel de Nantes

Il n'est pas banal qu'une juridiction suprême nationale invite directement une juridiction européenne à reconsidérer sa jurisprudence la plus récente. Un authentique dialogue des juges le justifie pourtant, lorsque les enjeux sont essentiels. Est-il déraisonnable d'envisager un revirement de la Cour de justice de l'Union européenne (CJUE) au sujet de la conservation des données de connexion, en réponse aux questions préjudicielles du Conseil d'Etat du 26 juillet 2018 ?

On sait que les données relatives au trafic des communications électroniques (« données de connexion ») ne permettent pas d'accéder au contenu de ces communications. Générées par l'utilisation des moyens de communication et nécessaires à des fins techniques ou de facturation par les opérateurs et fournisseurs d'accès à Internet, ces données comprennent principalement celles visant à localiser et identifier l'auteur et le destinataire d'une communication (nom, adresse, numéro de téléphone ou adresse IP), ainsi que des données sur la communication elle-même (date, durée et type) et sur le matériel utilisé. Prises dans leur ensemble et sur une longue période, elles permettent de tirer des conclusions précises sur la vie privée des utilisateurs des moyens de communication électronique - c'est-à-dire presque tout le monde. On comprend dès lors pourquoi les autorités publiques ont estimé nécessaire de pouvoir accéder, à des fins pénales ou administratives, à ces données conservées par les opérateurs - nourrissant ainsi des craintes liées à une nouvelle forme de « surveillance de masse ».

En France, le législateur a, dès la loi n° 2001-1062 du 15 novembre 2001, imposé aux opérateurs la conservation de ces données de connexion pour une durée maximale d'un an, afin de les rendre disponibles pour l'autorité judiciaire en vue de la recherche, de la constatation et de la poursuite des infractions pénales (code des postes et des communications électroniques [CPCE], art. L. 34-1). Par la suite, un accès administratif à ces données de connexion a été reconnu au profit de diverses administrations : administrations financières, services de la police et de la gendarmerie nationale, Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet (HADOPI), services de renseignement. S'agissant de ces derniers, la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a procédé à un meilleur encadrement de leur accès aux données de connexion, avec le renforcement des pouvoirs de contrôle d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement (CNCTR), et la création d'une procédure juridictionnelle spécifique devant une formation spécialisée du Conseil d'Etat (CJA, art. L. 311-4-1). Le législateur impose également aux fournisseurs d'accès à Internet et hébergeurs de conserver et mettre à la disposition de l'autorité judiciaire « 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 » (L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 6).

Parallèlement, l'Union européenne a adopté une directive 2006/24/CE du 15 mars 2006 visant à harmoniser partiellement les législations des Etats membres afin qu'ils imposent aux fournisseurs de communications électroniques de conserver les données de connexion pendant une période comprise entre six mois et deux ans.

Un dialogue des juges s'est engagé entre les juges nationaux et la CJUE sur la conformité au droit de l'Union de la conservation des données de connexion (v., not., sur cet historique, F.-X. Bréchot, Clap de fin pour la conservation généralisée des données de connexion en Europe ?, Rev. UE 2017. 178). Par un premier arrêt *Digital Rights Ireland*, la CJUE, saisie à titre préjudiciel par des juridictions irlandaise et autrichienne, a déclaré invalide la directive 2006/24/CE au motif que le législateur de l'Union avait par

ce texte porté une atteinte disproportionnée au droit au respect de la vie privée et au droit 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 (CJUE 8 avr. 2014, aff. C-293/12, AJDA 2014. 773 ; et 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1355, et les obs., note C. Castets-Renard ; et 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; RTD eur. 2015. 117, étude S. Peyrou ; et 168, obs. F. Benoît-Rohmer ; et 786, obs. M. Benlolo-Carabot). La rédaction de cet arrêt laissait néanmoins planer un doute quant à la compatibilité avec le droit de l'Union du principe même de la conservation généralisée des données de connexion. Ce doute a été levé par l'arrêt *Tele 2 Sverige et Watson* de la CJUE laquelle, sollicitée à titre préjudicielle par des juridictions suédoise et britannique, a condamné le principe même d'une telle conservation généralisée, à des fins de lutte contre la criminalité, tout en autorisant une conservation ciblée sous réserve qu'elle soit assortie de strictes garanties (CJUE 21 déc. 2016, aff. C-203/15, AJDA 2016. 2466 ; et 2017. 1106, chron. E. Broussy, H. Cassagnabère, C. Gänser et P. Bonneville ; D. 2017. 8 ; et 2018. 1033, obs. B. Fauvarque-Cosson et W. Maxwell ; Dalloz IP/IT 2017. 230, obs. D. Forest ; RTD eur. 2017. 884, obs. M. Benlolo Carabot ; et 2018. 461, obs. F. Benoît-Rohmer ; Rev. UE 2017. 178, étude F.-X. Bréchot ; JCP Adm. 2017, n° 27, p. 34, note C. Grossholz).

Il est peu de dire que l'arrêt *Tele 2 Sverige* a été mal reçu par les autorités nationales. La Commission européenne et quinze Etats membres intervenants avaient unanimement demandé à la Cour d'admettre la possibilité d'une conservation généralisée de ces données, sous réserve d'un encadrement strict de leur accès par les autorités publiques. Son avocat général, M. Henrik Saugmandsgaard Øe, concluait également en ce sens. Tous soulignaient que la conservation générale et indifférenciée, pendant une certaine durée, des données de connexion de l'ensemble des utilisateurs des moyens de communications électroniques constitue pour les Etats membres un outil décisif pour réprimer ou prévenir les infractions les plus graves, en particulier les actes terroristes. Cette conservation généralisée permet en effet aux enquêteurs, une fois la menace caractérisée ou réalisée, de « lire le passé » en accédant rétrospectivement aux données générées par les personnes mises en cause, y compris celles correspondant à la période durant laquelle ces personnes n'avaient pas encore été détectées comme présentant une menace grave pour la sécurité publique ou comme susceptibles de réaliser une infraction grave. L'accès à ces données joue ainsi très souvent un rôle déterminant pour l'identification, par l'autorité judiciaire ou les services administratifs compétents, des auteurs, des complices, des filières et des modes d'action des infractions graves ou actes terroristes. Il a pu être souligné que la « conservation ciblée » permise par la CJUE, consistant à n'autoriser que la conservation de certaines données générées par le seul « public dont les données sont susceptibles de révéler un lien, au moins indirect avec des actes de criminalité grave » ou de « prévenir un risque grave pour la sécurité publique » (pt 111 de l'arrêt *Tele 2 Sverige*), était impraticable et réduisait considérablement l'utilité de cet outil, du fait de la difficulté ou de l'impossibilité d'identifier à l'avance le « public » en cause, ainsi que de pouvoir remonter suffisamment dans le temps en l'absence de conservation imposée pour une certaine durée (v., not., F.-X. Bréchot, préc. ; C. Grossholz, préc.).

On comprend dès lors que le Conseil d'Etat, amené à se prononcer sur différents litiges dans lesquels était en jeu la conventionalité de la législation française au regard du droit de l'Union tel qu'interprété par la CJUE, ait décidé de poursuivre un dialogue des juges qui aurait pu sembler clos.

Le Conseil d'Etat était saisi, par plusieurs associations de défense des libertés sur Internet et un fournisseur d'accès à Internet, de recours pour excès de pouvoir dirigés contre deux séries d'actes administratifs. D'une part, sous les n^{os} 394922, 394925, 397844, 397851 (*Quadrature du Net et autres et Igwan.net*), était contestée la légalité de quatre décrets pris pour l'application de la loi du 24 juillet 2015 relative au renseignement, à savoir les décrets relatifs aux techniques de recueil de renseignement (décr. n° 2016-67 du 29 janv. 2016) et au contentieux de la mise en oeuvre de ces techniques (décr. n° 2015-1211 du 1er oct. 2015), ainsi que les décrets portant désignation des services spécialisés de renseignement (décr. n° 2015-1185 du 28 sept. 2015) ou des autres services autorisés à recourir à certaines de ces techniques (décr. n° 2015-1639 du 11 déc. 2015). D'autre part, sous le n° 393099 (*French Data Network e.a.*), était attaqué un refus d'abrogation de deux textes réglementaires précisant les conditions d'application de l'obligation pesant sur les opérateurs de communications électroniques de conserver les données de connexion de leurs clients (CPCE, art. R. 10-13) et de celles pesant sur les

fournisseurs d'accès à Internet et hébergeurs de conserver, pour les besoins de l'autorité judiciaire, les données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (décr. n° 2011-219 du 25 févr. 2011).

Devant faire application d'un arrêt de la CJUE qui n'emportait manifestement pas sa conviction, le Conseil d'Etat avait le choix entre trois solutions : la soumission, la rébellion ou la discussion. Il aurait pu choisir de se soumettre loyalement, par discipline juridictionnelle, à l'autorité de la chose jugée par la CJUE - c'est-à-dire, à défaut d'adhésion, opter pour une forme de soumission mêlée de résignation. Mais ce choix aurait conduit à affaiblir considérablement l'efficacité de la lutte contre le terrorisme sur le territoire français. Une entrée en rébellion l'aurait conduit à juger que les particularités du contexte français - « marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste », selon les décisions commentées - justifiaient de ne pas appliquer la jurisprudence de la CJUE, en tant qu'elle interdisait la conservation généralisée des données de connexion. Une telle solution aurait initié une rupture frontale avec le mouvement de rapprochement jurisprudentiel engagé depuis une quinzaine d'années par le Conseil d'Etat avec la CJUE. Fort heureusement, les juges du Palais-Royal, qui assument désormais un « dialogue des juges décomplexé » (G. Odinet et S. Roussel, AJDA 2017. 740), ont privilégié la poursuite de celui-ci avec les juges de Luxembourg, dans l'espoir de les convaincre d'amender leur jurisprudence *Tele 2 Sverige*. Cet espoir est partagé par d'autres : une juridiction britannique a renvoyé le 31 octobre 2017 à la CJUE des questions similaires (aff. C-623/17).

En adressant cinq questions préjudicielles à la CJUE et en soumettant à son appréciation, pour la première fois, la législation française relative à l'accès aux données de connexion, le Conseil d'Etat invite ainsi les juges de Luxembourg à reconsidérer leur jurisprudence *Tele 2 Sverige*, ainsi qu'à se prononcer sur des questions nouvelles. Les décisions commentées sont également intéressantes pour les questions qu'elles ont d'ores et déjà tranchées.

I - Les questions tranchées

Trois questions ont déjà été tranchées par les décisions commentées ou par des décisions antérieures : la conformité à la Constitution des diverses techniques de recueil de renseignement, la compatibilité avec la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Conv. EDH) des dispositions législatives françaises relatives à la conservation et au traitement des données de connexion et la délimitation de celles de ces dispositions qui entrent dans le champ d'application du droit de l'Union.

A. La conformité à la Constitution des diverses techniques de recueil de renseignement

Compte tenu du monopole du Conseil constitutionnel pour contrôler la conformité des lois à la Constitution, les décisions commentées ne comportent fort logiquement que peu de développements sur la constitutionnalité des dispositions législatives qui prévoient la conservation de certaines données et leur accès par les autorités publiques.

Dans l'affaire *French Data Network*, aucune question prioritaire de constitutionnalité (QPC) n'avait été posée par les requérants pour contester la conformité aux droits et libertés que la Constitution garantit des dispositions législatives que les actes réglementaires dont l'abrogation était demandée avaient pour objet d'appliquer. L'article L. 34-1 du CPCE impose aux opérateurs de communications électroniques de conserver les données de connexion de leurs utilisateurs aux fins, principalement, de les rendre disponibles à l'autorité judiciaire « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ». Ses dispositions n'ont, à notre connaissance, pas encore été soumises au contrôle du Conseil constitutionnel et auraient, dès lors, pu faire l'objet d'une QPC. En revanche, les dispositions du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 ont déjà été déclarées conformes à la Constitution (Cons. const. 10 juin 2004, n° 2004-496 DC, AJDA 2004. 1534, note J. Arrighi de Casanova) ; elles n'auraient dès lors pu, sauf changement de circonstances, être soumises de nouveau à l'examen du Conseil constitutionnel (ord. n° 58-1067 du 7 nov. 1958, art. 23-2).

Dans l'affaire *Quadrature du Net*, une QPC portant sur l'article 811-5 du code de la sécurité intérieure (CSI), relatif aux mesures de surveillance et de contrôle des transmissions empruntant la voie

hertzienne, avait été posée et renvoyée au Conseil constitutionnel par le Conseil d'Etat. Par sa décision du 21 octobre 2016 (n° 2016-590 QPC, AJDA 2017. 752, note E. Debaets ; D. 2016. 2120 ; et 2017. 1328, obs. N. Jacquinot et R. Vaillant ; Constitutions 2016. 653, chron. O. Le Bot ; et 713, chron.), le Conseil constitutionnel a déclaré cet article contraire au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

Néanmoins, le Conseil d'Etat considère que la déclaration d'inconstitutionnalité de cet article est sans incidence sur l'issue des litiges dirigés contre les quatre décrets d'application de la loi relative au renseignement. Cette solution peut, de prime abord, surprendre au regard de la jurisprudence du Conseil constitutionnel (Cons. const. 25 mars 2011, n° 2010-108 QPC, AJDA 2011. 647), appliquée par le Conseil d'Etat (CE, ass., 13 mai 2011, n° 316734, *M^me^ M'Rida*, Lebon avec les concl. ; AJDA 2011. 1136, chron. X. Domino et A. Bretonneau ; RFDA 2011. 789, concl. E. Geffray ; 806, note M. Verpeaux ; et 2012. 455, chron. H. Labayle, F. Sudre, X. Dupré de Boulois et L. Milano), selon laquelle, « en principe, la déclaration d'inconstitutionnalité doit bénéficier à l'auteur » de la QPC, sauf si le Conseil constitutionnel en a décidé autrement - ce qui n'était pas le cas en l'espèce. Le Conseil constitutionnel avait seulement décidé de reporter au 31 décembre 2017 la date de l'abrogation de la disposition contestée, tout en définissant, par une réserve d'interprétation, certaines garanties pour son application temporaire. Pour autant, le Conseil d'Etat avait déjà jugé par le passé que l'absence, dans la décision du Conseil constitutionnel, de prescriptions relatives à la remise en cause des effets produits par la disposition législative avant son abrogation doit être regardée comme indiquant qu'il n'a pas entendu remettre en cause ces effets antérieurs à l'abrogation avec effet différé, y compris à l'égard de l'auteur de la QPC, dans le cas particulier où elle a été soulevée à l'occasion d'un recours pour excès de pouvoir dirigé contre un acte réglementaire (CE 14 nov. 2012, n° 340539, *Association France nature environnement*, Lebon T. ; AJDA 2012. 2193 ; et 2373, chron. X. Domino et A. Bretonneau). Il a donc fait application de cette jurisprudence.

Par ailleurs, les requérants n'auraient pas pu poser de QPC relatives aux autres techniques de recueil de renseignement, dès lors qu'elles auraient été vouées au rejet, sauf changement de circonstances, en raison des décisions antérieures du Conseil constitutionnel.

Ce dernier a, en effet, lors de l'examen de la loi du 24 juillet 2015 relative au renseignement (Cons. const. 23 juill. 2015, n° 2015-713 DC, AJDA 2015. 1513 ; D. 2016. 1461, obs. N. Jacquinot et A. Mangiavillano), validé les conditions d'utilisation de la plupart de ces techniques : réquisition administrative des données de connexion (CSI, art. L. 851-1), transmission en temps réel de ces données à l'administration (CSI, art. L. 851-2 et L. 851-4), mise en place sur les réseaux des opérateurs d'algorithmes, paramétrés par les services de renseignement, de nature à détecter des connexions susceptibles de révéler une menace terroriste (CSI, art. L. 851-3), pose d'une « balise espion » permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet (CSI, art. L. 851-5), utilisation d'un *IMSI catcher* (système qui permet, par une antenne-relais fictive, d'intercepter toutes les connexions à une antenne réelle dans un périmètre restreint : CSI, art. L. 851-6), interceptions administratives de sécurité (qui permettent, sans le consentement des personnes concernées, d'avoir accès au contenu des communications émises : CSI, art. L. 852-1), dispositif de sonorisation de certains lieux et véhicules et captation d'images et de données informatiques stockées dans un système informatique (CSI, art. L. 853-1 à L. 853-3) et, enfin, mesures de surveillance des communications électroniques internationales (CSI, art. L. 854-1).

Dans cette même décision, le Conseil constitutionnel a en revanche jugé contraire à la Constitution, avant leur entrée en vigueur, les dispositions relatives à la procédure dite « d'urgence opérationnelle » (alors prévue au CSI, art. L. 821-6) et aux mesures de surveillance internationale (CSI, art. L. 854-1). La censure de ces dernières a nécessité une nouvelle intervention du législateur par la loi n° 2015-1556 du 30 novembre 2015, déclarée conforme à la Constitution (Cons. const. 26 nov. 2015, n° 2015-722 DC, AJDA 2015. 2298 ; D. 2016. 1461, obs. N. Jacquinot et A. Mangiavillano).

Par d'autres décisions, le Conseil constitutionnel a censuré les dispositions qui permettaient à diverses autorités administratives d'accéder aux données de connexion, à savoir l'Autorité de la concurrence

(Cons. const. 5 août 2015, n° 2015-715 DC, consid. 134 à 138, AJDA 2015. 1570), l'Autorité des marchés financiers (Cons. const. 21 juill. 2017, n° 2017-646/647 QPC, AJDA 2017. 2234 ; D. 2017. 1527 ; Rev. sociétés 2017. 582, note N. Martial-Braz ; RSC 2018. 496, obs. J.-M. Brigant) et la Haute autorité pour la transparence de la vie publique (Cons. const. 8 sept. 2017, n° 2017-753 DC, consid. 57 à 60, AJDA 2017. 1692). Il a également jugé contraire à la Constitution le dispositif d'accès administratif en temps réel aux données de connexion, prévu pour la prévention du terrorisme, en tant qu'il s'appliquait aux personnes appartenant à l'entourage d'une personne préalablement identifiée comme susceptible d'être en lien avec une menace terroriste, faute pour le législateur d'avoir prévu que le nombre d'autorisations simultanément en vigueur soit limité (Cons. const. 4 août 2017, n° 2017-648 QPC, AJDA 2017. 1642). Le législateur en a tiré les conséquences en modifiant le dispositif par la loi n° 2017-1510 du 30 octobre 2017, qui n'a pas été déférée au Conseil constitutionnel.

B. La compatibilité avec la convention

Sans surprise, le Conseil d'Etat, dans les décisions commentées, écarte l'exception d'inconventionnalité au regard de la convention européenne des droits de l'homme des dispositions législatives sur la base desquelles ont été pris les actes réglementaires ou refus d'abroger contestés.

Ainsi, dans l'affaire *French Data Network* (pt 5), il juge que le fait que l'obligation de conservation des données de connexion imposée aux opérateurs revête un caractère général, sans être limitée à des personnes ou circonstances particulières, n'est pas, par lui-même, contraire aux exigences découlant de l'article 8 de la Conv. EDH. En effet, la Cour européenne des droits de l'homme n'a jamais eu l'occasion de se prononcer directement sur la conservation généralisée des données de connexion et ne l'a, dès lors, jamais condamnée. Tout au plus peut-on relever que, chaque fois qu'elle a été saisie de mesures nationales de surveillance secrètes, la Cour de Strasbourg s'est livrée à une analyse de l'ensemble des garanties entourant ces mesures afin d'apprécier leur conformité aux articles 8 et 13 de la Conv. EDH (v., par ex., CEDH 4 déc. 2015, n° 47143/06, *Zakharov c/ Russie* ; ou CEDH 12 janv. 2016, n° 37138/14, *Szabó et Vissy c/ Hongrie*, AJDA 2016. 1738, chron. L. Burgorgue-Larsen ; CEDH 19 juin 2018, n° 35252/08, *Case of Centrum för Rättvisa c/ Suède*).

Par ailleurs, la décision *Quadrature du Net* considère (pts 7 à 11) que les conditions de saisine de la formation spécialisée du Conseil d'Etat ainsi que celles dans lesquelles elle remplit son office juridictionnel (avec notamment de fortes dérogations apportées au principe du contradictoire, contrebalancées par de larges pouvoirs d'instruction, d'examen d'office des moyens de légalité et d'injonction d'office à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées) sont compatibles avec le droit au recours effectif des personnes qui la saisissent, garanti par l'article 13 de la Conv. EDH.

Enfin, cette même décision précise (pts 12 et 13) que la circonstance que la loi ne prévoie pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet, une fois ces mesures levées, ne caractérise pas, par elle-même, une atteinte excessive portée au droit au respect de la vie privée garanti par l'article 8 de la Conv. EDH, ainsi que l'a d'ailleurs jugé la Cour de Strasbourg (arrêt *Zakharov c/ Russie*, préc., § 287). Pour parvenir à cette conclusion, le Conseil d'Etat met en exergue les attributions de la CNCTR et le recours effectif ouvert devant la formation spécialisée du Conseil d'Etat, dont on peut penser qu'elles sont de nature à garantir le respect des droits des personnes concernées, tout en préservant le secret de la défense nationale et l'efficacité des mesures nécessaires à la sécurité nationale.

C. La délimitation des techniques qui entrent dans le champ d'application du droit de l'Union

Le dernier point intéressant tranché par les décisions commentées est la délimitation des dispositions françaises qui relèvent du champ d'application du droit de l'Union, et donc de la charte des droits fondamentaux, en application de l'article 51, § 1, de celle-ci.

Le Conseil d'Etat identifie deux directives dont le champ d'application est susceptible de couvrir les dispositions législatives contestées par la voie de l'exception.

Il s'agit, tout d'abord, de la directive 2002/58/CE du 12 juillet 2002 dite « Vie privée et communications électroniques ». Alors même que l'article 1er, § 3, de celle-ci dispose qu'elle ne s'applique pas aux activités concernant notamment la sûreté de l'Etat et le droit pénal, son article 15, § 1, contient une disposition permissive autorisant les Etats membres, pour des motifs tenant notamment à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à déroger à diverses obligations prévues par la directive (dont celles de confidentialité des données de connexion). Dans son arrêt *Tele 2 Sverige*, la CJUE a considéré, ce qui n'allait pas de soi, que la directive s'appliquait tant aux mesures nationales qui prévoient l'obligation des fournisseurs de conserver les données de connexion qu'à celles qui prévoient leur accès par les autorités nationales.

Dans sa décision *Quadrature du Net* (pts 18 à 21), le Conseil d'Etat prend acte de cette interprétation : la directive « doit être regardée comme régissant les activités des fournisseurs [de services de communications électroniques] ». Il en déduit, *a contrario*, que « les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en oeuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive » (pt 18).

Par conséquent, faisant application de la théorie de l'acte clair, le Conseil d'Etat juge que trois séries de dispositions relèvent du champ d'application de l'article 15, § 1, de la directive 2002/58/CE : l'obligation de conservation des données de connexion, les accès administratifs à ces données, y compris en temps réel (CSI, art. L. 851-1, L. 851-2 et L. 851-4), et la mise en place sur les réseaux des opérateurs d'algorithmes de nature à détecter des connexions susceptibles de révéler une menace terroriste (CSI, art. L. 851-3).

En revanche, il considère que ne relèvent pas du champ d'application de cette directive la pose d'une « balise espion » (CSI, art. L. 851-5), l'utilisation d'un *IMSI catcher* (CSI, art. L. 851-6), les interceptions administratives de sécurité (CSI, art. L. 852-1 et s.), la sonorisation de certains lieux et véhicules et la captation d'images et de données informatiques (CSI, art. L. 853-1 à L. 853-3) et les mesures de surveillance des communications électroniques internationales (CSI, art. L. 854-1).

L'autre texte identifié par le Conseil d'Etat comme susceptible de faire entrer le droit français dans le champ d'application du droit de l'Union, et donc de la charte, est la directive 2000/31/CE du 8 juin 2000, dite « sur le commerce électronique ». Dans sa décision *French Data Network* (pts 12 à 14), il considère que les dispositions du II de l'article 6 de la loi du 21 juin 2004, qui imposent une obligation de détention et de conservation des seules données relatives à la création de contenu, n'entrent pas dans le champ d'application de la directive 2002/58/CE mais relèvent de façon claire de celui de la directive 2000/31/CE.

II - Les questions en suspens

Certaines questions préjudicielles renvoyées par le Conseil d'Etat portent sur des sujets déjà abordés par la CJUE, qui est ainsi invitée à amender sa jurisprudence, d'autres sont inédites.

A. Des questions renouvelées

Par trois questions, dont deux similaires, le Conseil d'Etat invite directement la CJUE à reconsidérer sa jurisprudence *Tele 2 Sverige*.

Les premières questions de chacune des décisions commentées sont les plus importantes. Le Conseil d'Etat demande à la CJUE d'interpréter l'article 15, § 1, de la directive 2002/58/CE comme autorisant les Etats membres à imposer aux fournisseurs une obligation de conservation généralisée et indifférenciée des données de connexion en vue de leur accès par, respectivement, les services de renseignement et l'autorité judiciaire. Le raisonnement qui les sous-tend se décline en trois temps.

D'une part, le Conseil d'Etat fait valoir que la conservation préventive et indifférenciée des données de connexion présente, pour la recherche et la poursuite des infractions pénales, ainsi que pour la prévention des atteintes à la sécurité nationale et, en particulier, du risque terroriste, « une utilité sans équivalent » par rapport à une conservation ciblée - c'est-à-dire au recueil de ces mêmes données à

partir seulement du moment où un individu est suspecté d'avoir commis une infraction pénale ou a été identifié comme susceptible de présenter une menace pour la sécurité nationale. Dès lors qu'il est impossible ou difficile d'identifier à l'avance ces personnes, la conservation ciblée présente une utilité très relative, faute de permettre de « remonter le temps » pour avoir accès aux données relatives aux communications effectuées par l'individu en cause avant sa détection.

D'autre part, le Conseil d'Etat invite la CJUE à ne pas se focaliser uniquement sur le principe d'une conservation généralisée des données de connexion mais à apprécier la proportionnalité de cette ingérence dans les droits fondamentaux « notamment eu égard aux garanties et contrôles » dont sont assortis l'accès à ces données et leur utilisation. Ainsi, il demande à la CJUE d'adopter une grille d'analyse similaire à celle de la Cour de Strasbourg, laquelle, loin de condamner par principe un dispositif de surveillance, même de masse, apprécie la conventionnalité de celui-ci au regard de l'ensemble des garanties qui l'assortissent. Cette analyse était aussi celle défendue par l'avocat général dans ses conclusions sur l'affaire *Tele 2 Sverige*, ainsi que par tous les Etats membres intervenants et la Commission. En outre, la décision *Quadrature du Net* souligne « le contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste ». Cette mention peut être lue comme une invitation faite aux juges de Luxembourg de mesurer les conséquences qui résulteraient, pour les Etats membres les plus menacés, de la privation de l'un des outils les plus précieux pour la prévention et la répression des actes terroristes. Elle peut aussi être interprétée en faveur d'une approche moins intégrationniste, plus adaptée à la nature et à l'intensité des menaces pesant sur les différents Etats membres. Une telle approche, plus respectueuse du principe de subsidiarité, consisterait à prendre en compte les circonstances de temps et de lieu pour autoriser certains Etats à prendre des mesures plus sévères que d'autres, dans la limite du strict nécessaire, compte tenu du contexte national. Le respect des droits fondamentaux pourrait en effet s'accommoder de dispositifs variés, adaptés aux traditions et contraintes de chaque Etat membre - avec évidemment le risque, hélas déjà vérifié, que certains actes terroristes soient préparés dans les Etats où les mesures de surveillance sont moindres.

Enfin, le Conseil d'Etat relève que la conservation généralisée des données de connexion, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « contenu essentiel » des droits consacrés par les articles 7 (respect de la vie privée) et 8 (protection des données à caractère personnel) de la charte - comme l'a déjà jugé la CJUE. Or, cette dernière a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017 (relatif à l'accord envisagé entre l'Union européenne et le Canada sur le transfert et le traitement des données des dossiers des passagers aériens, dites « PNR »), « qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux » et que « la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui », en particulier le droit à la sûreté garanti par l'article 6 de la charte. De surcroît, le Conseil d'Etat rappelle qu'en vertu de l'article 4 du TUE, l'Union « respecte les fonctions essentielles de l'Etat, notamment celles qui ont pour objet [...] de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque Etat membre ». Ce qui signifie non seulement que l'Union n'est pas compétente pour prendre des mesures qui relèvent de la sécurité nationale, mais aussi qu'elle ne devrait pas porter atteinte à la capacité des Etats membres à préserver leur sécurité nationale.

Par ailleurs, la troisième question de la décision *Quadrature du Net* revient à inviter la CJUE, dans la lignée de la jurisprudence de la Cour de Strasbourg (v. *supra*), à ne plus considérer comme systématiquement nécessaire d'informer les personnes concernées par une mesure de surveillance par les services de renseignement, une fois qu'une telle information n'est plus susceptible de compromettre les enquêtes - étant précisé que la législation française ne prévoit pas une telle information. La CJUE est invitée à juger que les procédures de recueil des données de connexion peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours.

B. Des questions nouvelles

Le Conseil d'Etat adresse enfin à la CJUE deux questions inédites.

La deuxième question de la décision *Quadrature du Net* est relative aux mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste. Ces mesures qui, en France, ne sont autorisées que pour les seuls besoins de la prévention du terrorisme, affectent les droits et obligations des fournisseurs d'un service de communications électroniques sans leur imposer pour autant une obligation spécifique de conservation de leurs données. Le Conseil d'Etat précise là aussi que « dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, [...] ces techniques présentent [...] une utilité opérationnelle sans équivalent ». Il demande donc à la CJUE si une réglementation nationale qui prévoit de telles mesures est autorisée par la directive 2002/58/CE, lue à la lumière de la charte.

Egalement inédite est la seconde question de la décision *French Data Network* relative à l'obligation qui pèse en France sur les fournisseurs d'accès à Internet et hébergeurs de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu des services dont elles sont prestataires, afin de les rendre disponibles pour l'autorité judiciaire. Le Conseil d'Etat demande si une telle législation est compatible avec les dispositions de la directive 2000/31/CE, lue à la lumière des articles 6, 7, 8, 11 et 52, § 1, de la charte.

Cette nouvelle illustration du « dialogue des juges décomplexé » trouvera-t-il un écho favorable du côté de Luxembourg ?

Mots clés :
DROIT EUROPEEN * Droit de l'Union européenne * Cour de justice de l'Union européenne * Question préjudicielle
DROITS FONDAMENTAUX ET PRINCIPES GENERAUX * Droits et libertés fondamentaux * Droit au respect de la vie privée * Données personnelles