Compte-rendu d'audience
CJUE, 9 et 10 septembre 2019, *Privacy International*, *La Quadrature du Net e.a.*, *French Data Network e.a.* et *Ordre des barreaux francophones et germanophone e.a.*, aff. C-623/17, C-511/18, C-512/18 et C-520/18

Bastien Le Querrec

17 septembre 2019

Les 9 et 10 septembre 2019 se tenait l'audience devant la CJUE dans les affaires *Privacy International*, *La Quadrature du Net e.a.*, *French Data Network e.a.* et *Ordre des barreaux francophones et germanophone e.a.* [1] Il s'agit de quatre affaires jointes car reposant sur le même sujet : la légalité des régimes de conservation des données de connexion pour des fins de renseignement. La Cour a posé plusieurs questions aux parties en amont de l'audience. Des observations écrites ont été produites pendant l'été et cette audience revenait dessus à travers plaidoiries, questions orales de la Cour puis répliques.

I. Présentation des litiges

Dans les quatre affaires, des questions préjudicielles ont été transmises à la Cour, lui demandant d'évaluer la conformité au droit de l'UE de mesures nationales de conservation généralisée des données de connexion.

Une donnée de connexion est ce qui englobe un message. On peut faire l'analogie avec une lettre dans une enveloppe : les données de connexion sont ce qu'il y a sur l'enveloppe et le contenu de la communication est ce qu'il y a à l'intérieur de l'enveloppe. Concrètement, sont des données de connexion le destinataire et l'expéditeur d'un message, l'adresse IP d'un

1. Le *leading case* est l'affaire de *Privacy International*, l'arrêt devrait donc porter ce nom.

terminal, la liste des antennes téléphoniques sur lesquelles un téléphone s'est connecté, etc. Il ne s'agit pas, en théorie, du contenu d'une conversation. Les associations à l'origine du litige ont cependant montré que cette distinction est souvent difficile à faire en pratique.

Pour des questions de lutte contre la criminalité ou de protection de la sécurité nationale, les États membres conservent ces données de connexion. En France, cette durée de conservation est d'un an (art. R. 10-13 CPCE). Dans les arrêts *Digital Rights Ireland* (CJUE, 8 avril 2014, aff. C-293/12 et C-594/12) et *Tele2 Sverige AB* (CJUE, 21 décembre 2016, aff. C-203/15 et C-698/15), la Cour avait considéré que le principe même d'une conservation généralisée des données de connexion était contraire à la Charte de l'UE.

En France, suite à l'arrêt *Digital Rights Ireland*, La Quadrature du Net et d'autres associations ont fait une demande d'abrogation de l'article R. 10-13 CPCE. Ce n'est que le 26 juillet 2018, par deux arrêts (aff. 394922 et 393099), que le Conseil d'État a posé cinq questions relatives à la conformité au droit de l'UE du droit français en matière de conservation des données de connexion.

Il faut distinguer la conservation et l'accès. Toutes les législations européennes imposent une conservation généralisée des données de connexion : les opérateurs sont tenus à une obligation de conservation, pendant une durée variable, des données de connexion de tous leurs utilisateurs. L'étendue de cette conservation généralisée varie en fonction de l'État : elle peut concerner toutes les données de connexion (par exemple en France), ou bien seulement certains types de données de connexion (par exemple en Suède dans sa réforme à venir). Les données conservées font, dans un deuxième temps, l'objet d'un accès. Cet accès est, en théorie, toujours limité, par exemple par l'obligation de motivation de la demande d'accès ou de vérification par une autorité de contrôle.

Les parties étaient invitées par la CJUE à revenir sur le champ d'application de la directive 2002/58 (*ePrivacy*) et l'applicabilité du droit de l'Union, sur l'effet dissuasif (*chilling effect*) d'une conservation généralisée au regard de la Charte, sur l'hypothèse d'un régime de conservation généralisée mais à l'accès ciblé, sur la comptabilité d'une analyse automatisée des données de connexion avec le droit à la vie privée, ou encore sur une modalité de conservation des données de connexion la moins attentatoire aux droits et libertés de la Charte.

II. Plaidoiries (premier jour)

A. Arguments des associations plaignantes

Les associations plaignantes estiment que les législations des États membres qui imposent une conservation généralisée des données de connexion ne respectent pas la Charte. L'argumentation reprend celle développée en 2016 dans l'affaire *Tele2* : la conservation généralisée est une ingérence disproportionnée aux droits protégés par la Charte.

Lors de l'audience, les associations plaignantes ont relevé que, tant pour le droit britannique, français ou belge, les données de connexion, mais aussi, dans certains cas, le contenu même des communications, sont visés par l'obligation de conservation faites aux opérateurs. Selon les plaignantes, les garanties au moment de l'accès à ces données sont insuffisantes, voire inexistantes.

La plaidoirie des associations françaises [2] a également critiqué les finalités assez larges et mal définies permettant de mettre en place des techniques de renseignement, qui comprennent l'accès aux données de connexion. Les plaignantes ont voulu démontrer qu'il existe en France une surveillance de masse : par ces finalités imprécises, l'accès aux données de connexion n'est pas limité. Combiné à une conservation généralisée, cet accès non limité participe à l'absence de proportionnalité du dispositif. La pratique de l'échange d'informations entre États constituerait également une surveillance de masse : l'encadrement des missions de renseignement est toujours plus laxiste en matière de surveillance extérieure ; les agences peuvent cependant obtenir, par le biais des coopérations entre États, des informations sur leurs propres citoyens récupérées par un État étranger, donc sous un régime plus laxiste de surveillance extérieure. C'est sur ce constat de surveillance de masse que les plaignantes ont ensuite détaillé les effets néfastes d'une telle conservation des données de connexion. Au-delà de l'absence de proportionnalité d'une telle obligation, les associations ont souligné les abus actuels de telles mesures : elles ont rappelé que, en France, les finalités du renseignement ont été détournées de leur objectif premier dans le cas des « gilets jaunes », et plus généralement dans le cas de contestations sociales. Les plaignantes sont revenues sur l'effet dissuasif de la surveillance de masse, citant plusieurs études sociologiques liées à la surveillance.

Les associations réclament une notification des personnes qui ont fait l'objet d'une surveillance. Le cas de la journaliste Camille Polloni a été cité : à la suite d'une procédure longue, fastidieuse et souvent incompréhensible vu de l'extérieur, la journaliste a pu prendre connais-

2. Les associations La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs et Igwan.net ayant le même avocat, celui-ci a répondu aux différentes questions posées par la Cour avant l'audience au travers de ses prises de paroles pour ses différentes clientes.

sance d'une mesure de surveillance illégale à son encontre par le renseignement militaire (sans savoir en quoi cette surveillance a consisté ni en quoi elle était illégale) et s'est vue assurée par le Conseil d'État que la demande de suppression des informations illégalement recueillies a bien été faite. Cet exemple fait dire aux plaignantes que la procédure actuelle devant le Conseil d'État n'est pas suffisante pour lever les craintes car elle n'est pas transparente. Seule une notification systématique permettrait de résoudre ce problème : autrement, les personnes sous surveillance ne peuvent pas savoir qu'elle l'ont été et ne peuvent pas faire protéger leurs droits en cas d'abus.

Les associations ont rappelé que le droit de l'UE s'appliquait. Par un raisonnement *a contrario*, elles ont voulu démontrer que si la directive *ePrivacy* ne s'appliquait pas, elle se retrouverait vidée de son sens. La sécurité nationale n'est pas, pour les plaignantes, source d'incompétence du droit de l'UE. Non seulement il s'agit toujours de mise en œuvre du droit du l'Union au sens de la jurisprudence *Pfleger* (CJUE, 30 avril 2014, aff. n° C-390/12), mais les législations nationales en question dépassent très largement la seule sécurité nationale.

Enfin, les associations plaignantes ont très vivement critiqué la formulation des questions posées par le Conseil d'État. Celles-ci seraient tournées de manière à demander à la Cour de revoir sa jurisprudence, ce qui ne serait pas le rôle du Conseil d'État.

Lors des répliques, La Quadrature du Net a insisté sur ce qui serait, selon elle, une solution satisfaisante au litige. Elle a non seulement demandé à la Cour de maintenir sa jurisprudence *Tele2*, mais aussi de préciser que seul un système de conservation spontanée des données de connexion, à la manière de ce qu'il se pratique aux États-Unis, permettrait d'avoir autant d'efficacité sans obligation de conservation généralisée des données de connexion (cf. *infra*).

B. Arguments des États membres, de la Commission européenne et du Contrôleur européen de la protection des données (CEPD)

Les États membres ont tous plaidé en faveur d'une conservation généralisée des données de connexion. Selon eux, la directive *ePrivacy* et la Charte UE ne peuvent s'appliquer au litige parce qu'on serait en matière de sécurité nationale, de compétence exclusive des États membres. Ils appellent à ne pas transposer la jurisprudence *Tele2* au domaine du renseignement.

Les États membres ont également, unanimement, indiqué que la jurisprudence *Tele2* ne pouvait être appliquée, et qu'ils ne voudront pas l'appliquer si elle était maintenue voire étendue aux activités de renseignement. Les plaidoiries des États membres étaient toutes accompagnées de nombreux exemples d'affaires criminelles qui étaient sensées illustrer la nécessité d'un régime de conservation généralisée des données de connexion. L'impression donnée était cependant que les États membres voulaient surtout jouer sur les émotions, tout comme *Child Focus*, une

association qui intervenait en soutien des obligations conservation généralisée et qui, dans ses exemples, a créé un malaise dans le public en raison de la manière dont les faits divers étaient racontés et des détails toujours plus sordides [3] [4]. Pourtant, ces exemples mélangeaient très souvent criminalité et sécurité nationale, ce que releva la Cour dans ses questions le deuxième jour.

Beaucoup d'États membres intervenaient surtout pour défendre leur législation nationale de conservation généralisée des données de connexion. Les garanties accordées au stade de l'accès ont fait l'objet de nombreux développements. On a ainsi pu retrouver régulièrement le fait qu'un juge ou une autorité administrative indépendante était chargée de contrôler les demandes d'accès aux données de connexion et vérifier que les conditions – strictes et nombreuses selon les États membres – étaient bien remplies. Notons que, sur le cas français, La Quadrature du Net et le gouvernement français s'opposent radicalement. La France affirme que le contrôle *a priori* et *a posteriori* est efficace, alors que La Quadrature a rappelé ses démonstrations devant le Conseil d'État de l'inefficacité du contrôle opéré par la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La jurisprudence de la CEDH, notamment *Big Brother Watch c. Royaume-Uni* (CEDH, 13 septembre 2018, *Big Brother Watch et autres*, 58170/13, 62322/14 et 24960/15) a été appelée par les États membres à l'appui d'une acceptation par la Cour de Strasbourg de mesures de surveillance. Les États membres ont demandé à la Cour de se conformer à cet arrêt.

Certains États membres comme la Suède estiment qu'il n'est pas nécessaire de faire une conservation généralisée et indifférenciée des données de connexion, mais seulement une conservation généralisée sur certains types de données de connexion. La Commission européenne et le Contrôleur européen de la protection des données (CEPD) partagent cette position [5] : selon eux, il faudrait une liste, exhaustive, de types de données de connexion qui pourraient faire l'objet d'une conservation généralisée. Cela exclurait ainsi, entre autres, les adresses des sites Web, sujet de discussion entre la France et La Quadrature du Net. La France ou le Royaume-Uni, notamment, se sont opposés à une conservation de certaines données de connexion uniquement et ont plaidé pour une conservation généralisée et indifférenciée.

Tous les États membres ont estimé que la seule solution alternative à la conservation généralisée serait une conservation ciblée, pour décrédibiliser immédiatement une telle hypothèse. Selon eux, une conservation ciblée doit se faire selon des critères obligatoirement discriminatoires voire portant atteinte à la présomption d'innocence (ce que ne ferait pas une conservation

3. L'avocate de l'association a décrit, entre autres, l'histoire d'une « *toute, toute petite fille, de 10 à 12 ans* », et d'un prédateur sexuel « *proche de son fantasme ultime* ».

4. *Child Focus* semblait également proche du gouvernement belge : le texte de la plaidoirie de cette association circulait parmi les membres du gouvernement belge, et la réplique a été préparée avec les agents belges.

5. La Commission a également rejoint la position des États membres sur l'inapplicabilité de *Tele2*, ce qui explique peut-être pourquoi elle n'a lancé aucune procédure en manquement.

généralisée et un accès ciblé). Cette hypothèse part du postulat, rappelé par le Royaume-Uni, que la conservation ou l'accès à des données de connexion ne crée pas du renseignement mais est seulement un préalable au renseignement. Ce faisant, les États membres ont, implicitement, rejeté l'hypothèse d'une conservation ciblée selon des critères tirés d'une surveillance préalable par d'autres techniques (individuelles) de renseignement. On aurait ainsi pu imaginer une conservation des données de connexion d'un individu ou groupe d'individus préalablement repérés comme présentant une menace éventuelle puis, après conservation, une analyse fine des données de connexion pour confirmer ou infirmer les craintes. Les États membres ont également rejeté cette hypothèse en précisant qu'un des objectifs des mesures de conservation et d'accès aux données de connexion est de détecter les menaces inconnues (les signaux faibles, indétectables par une analyse exclusivement humaine).

III. Questions de la Cour (deuxième jour)

La deuxième journée était consacrée aux questions de la Cour, d'abord le juge rapporteur, puis l'avocat général, suivis des autres juges de la formation de jugement. Le juge rapporteur est le même que dans *Tele2*.

L'impression qui ressort des questions posées par la Cour est que celle-ci fait très attention à ne pas tomber dans la vision sécuritaire des États membres. De nombreuses prises de paroles des juges ont fait ressortir les contradictions des États membres. Le président et l'avocat général semblaient agacés par les plaidoiries des gouvernements de la veille qui se répétaient. Le juge rapporteur a rappelé que l'arrêt *Big Brother Watch*, utilisé très régulièrement par les États membres pour soutenir qu'une mesure de conservation généralisée des données de connexion ne serait pas contraire à la CEDH, n'est pas définitif, et l'avocat général a mis en difficulté les États membres sur la pertinence de leurs exemples qui ne portaient que très rarement sur la sécurité nationale. À plusieurs reprises, la Cour a rappelé les craintes émises par la commission de Venise à propos d'une conservation généralisée des données de connexion.

La Commission et la France ont régulièrement été mises en difficulté par les questions du juge rapporteur et de l'avocat général. Ils ne semblaient pas convaincus par le raisonnement des États membres sur la proportionnalité d'un régime de conservation généralisée avec accès ciblé. Le juge rapporteur a par exemple demandé à la Commission s'il n'y aurait pas renversement entre la règle et l'exception en termes de protection de la vie privée si on acceptait un tel régime. La France n'a pas été capable d'expliquer comment on pourrait avoir une analyse des données de connexion par la surveillance algorithmique (les « boites noires ») sans avoir également une analyse du contenu de la communication elle-même [6]. Le juge rapporteur a également rejeté

6. Sur ce point, La Quadrature du Net avait déjà expliqué devant les tribunaux français qu'il n'est pas tech-

l'argument des États membres consistant à opposer conservation généralisée et conservation ciblée, cette dernière n'étant pas la seule solution alternative à une conservation généralisée. La France n'a pas été capable d'indiquer à l'avocat général quels types de données de connexion il faudrait impérativement inclure dans la liste exhaustive proposée par la Commission pour ne plus faire de conservation indifférenciée, tout en reconnaissant qu'une telle liste pourrait, par exemple, exclure les adresses des sites Web.

La Cour a également cherché à connaître les conséquences tirées par la Commission et le CEPD de l'arrêt *Digital Rights Ireland*. La Cour a rappelé qu'elle affirmait dans *Digital Rights Ireland* que rien ne permet de conclure à la nécessité d'avoir une conservation généralisée pour remplir les objectifs de lutte contre la criminalité. Elle a ensuite demandé à la Commission puis au CEPD si des études ont été menées suite à cet arrêt, et si elles viendraient conclure à la nécessité d'une conservation généralisée. Mais aucune étude n'a été faite par la Commission ou le CEPD.

Enfin, l'avocat général a demandé aux associations plaignantes des précisions sur le régime américain de conservation des données de connexion. Suite à cette question, la réplique de La Quadrature du Net s'est notamment concentrée sur la solution que serait un régime de conservation spontanée des données de connexion inspiré du modèle américain. La conservation spontanée des données de connexion repose sur le postulat que les opérateurs conservent nécessairement certaines données de connexion pour des raisons légitimes (notamment facturation et protection des infrastructures) et propres à leurs activités (tous les opérateurs n'ont pas la même activité, donc ne conservent pas les mêmes types de données de connexion pour cela). Un régime de conservation spontanée des données de connexion permettrait, selon La Quadrature du Net, de ne pas imposer une conservation généralisée ni une conservation différenciée (cf. *supra*), donc être compatible avec la jurisprudence *Tele2* de la CJUE tout en offrant une efficacité similaire au modèle allemand qui se rapproche le plus de ce qu'il se fait aux États-Unis [7].

IV. Suites du litige

Les conclusions de l'avocat général sont attendues pour fin décembre 2019 ou début janvier 2020. L'arrêt de la CJUE arrivera quelques mois après. La Cour, à travers ses questions, semble se diriger vers la constatation que le droit de l'Union est applicable à la sécurité nationale et

niquement possible de ne pas analyser le contenu des communications avec une surveillance algorithmique des données de connexion : pour accéder aux données de connexion, les « boites noires » doivent également analyser le contenu des communication pour extraire les données de connexion.

7. Le modèle allemand repose lui aussi sur une obligation de conservation généralisée des données de connexion, mais cette obligation est beaucoup plus légère qu'en France, et ne concerne notamment pas les accès à des fins de renseignement, comme précisé par le gouvernement allemand dans sa réplique.

un maintien d'une interdiction de conservation généralisée et indifférenciée des données de connexion.

En revanche, il est possible qu'elle accepte une conservation généralisée de certains types de données de connexion uniquement (la conservation ne serait alors plus indifférenciée), comme ce que demandent la Commission, le CEPD ou certains États membres comme la Suède. Il est aussi possible que la position de La Quadrature du Net, qui consiste à interdire toute conservation généralisée, même différenciée, soit maintenue avec comme seule solution possible une législation reposant sur la conservation spontanée des données de connexion.

Mise à jour du 18 septembre : French Data Network était présentée, à tort, comme ayant le même avocat que La Quadrature du Net.