Affaires C-511/18 et C-512/18

Fédération des fournisseurs d'accès à Internet associatifs

Le 27 novembre 2018

Table des matières

1 Introduction **2**

2 La conservation généralisée imposée aux opérateurs **3**
2.1 La sécurité nationale ne justifie pas l'obligation 4
2.1.1 La lutte contre le terrorisme ne relève pas de la sécurité nationale 4
2.1.2 L'obligation s'apprécie au regard de toutes les finalités poursuivies 5
2.1.3 L'évolution du contexte ne justifie pas l'obligation 7
2.2 Aucune garantie ni aucun contrôle ne peut justifier l'obligation 8
2.2.1 Le droit français ne respecte déjà pas le droit de l'Union 8
2.2.2 L'obligation n'est pas nécessaire 10

3 La conservation généralisée imposée aux hébergeurs **11**
3.1 La directive 2002/58 s'applique aux hébergeurs 12
3.2 L'obligation imposée aux hébergeurs est tout autant disproportionnée que celle imposée aux opérateurs 13
3.2.1 Une symétrie déjà reconnue en matière de surveillance active . . . 13
3.2.2 Une ingérence tout aussi importante s'agissant de l'adresse IP . . 14
3.2.3 Une ingérence plus importante s'agissant des autres informations . 14
3.2.4 L'obligation n'est pas nécessaire 15

1 Introduction

1 Le Conseil d'État a transmis à la Cour de justice de l'Union européenne cinq questions préjudicielles.

2 Trois de ces questions concernent la conformité au droit de l'Union européenne des dispositions françaises qui imposent aux intermédiaires techniques de conserver pendant un an des **données de connexion** concernant l'ensemble de leurs utilisateurs. Il s'agit des deux questions transmises dans l'affaire C-512/18 et de la première question transmise C-511/18. Elles seront traitées dans les présentes écritures.

3 Deux autres questions concernent la conformité au droit de l'Union européenne du cadre, plus large, des **activités étatiques de surveillance**, couvrant les mesures directement mises en œuvre par l'État ainsi que l'effectivité des recours prévus contre ces mesures. Il s'agit des deuxième et troisième questions transmises dans l'affaire C-511/18. Elles sont traitées par La Quadrature du Net dans ses propres écritures.

4 À titre liminaire il convient de souligner le contexte dans lequel ces questions ont été posées, notamment au regard de la jurisprudence développée par la Cour de justice dans ses arrêts Digital Rights Ireland [1], Schrems [2] et Tele2 [3]. Lors de la séance publique du 11 juillet 2018 devant le Conseil d'État, le rapporteur public, M. Édouard Crépey considérait que :

> *« L'honnêteté oblige à le reconnaître d'emblée : quels que soient les efforts argumentatifs du premier ministre en défense, nul ne peut sérieusement contester que l'application disciplinée de la jurisprudence de la CJUE devrait vous conduire à annuler ces refus d'abroger comme pris sur la base de dispositions législatives contraires aux exigences du droit de l'Union. »*

5 Et d'ajouter :

> *« Il y a donc tout lieu de penser qu'appliquée fidèlement, la jurisprudence Tele2 Sverige AB rend illégaux les refus d'abroger attaqués. Faut-il toutefois appliquer cette jurisprudence ? Nous en arrivons au cœur de la question. Or l'appréciation de la Cour est à notre sens gravement déséquilibrée et nous vous proposons en conséquence de l'inviter à réexaminer sa position en lui posant une question préjudicielle. [...] si votre conviction est que la Cour a inexactement pesé les différents éléments du débat, il y a lieu pour vous de lui demander de réexaminer sa position. Or telle est bien la situation à nos yeux. Et en restant même, à ce stade, à la seule question de l'article R. 10-13 du CPCE et du décret du 27 février 2011, c'est-à-dire aux obligations de conservation liées aux seules nécessités des enquêtes pénales conduites par l'autorité judiciaire, nous peinons à penser que les auteurs de la directive 2002/58, même éclairés rétrospectivement par les exigences de la Charte, aient entendu y faire obstacle. »*

1. CJUE, grande chambre, 8 avril 2014, Digital Rights Ireland et autres, C-293/12, C-594/12
2. CJUE, grande chambre, 6 octobre 2015, Schrems, C-362/14
3. CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige, Watson et autres, C-2013/15, C-698/15

6 En outre, il invitait clairement le Conseil d'État à s'éloigner de la jurisprudence de la Cour de justice : *« Nous ne saurions vous dissimuler que nous nous séparons sur ce point d'une mention de l'arrêt Tele2 Sverige AB (§ 77) selon laquelle toute mesure prise par toute personne autre que les utilisateurs qu'il s'agisse d'entités privées ou d'entités étatiques, et portant atteinte à la confidentialité des communications électroniques serait dans le champ de la directive mais c'est là une nuance que nous vous invitons à assumer en tranchant vous-mêmes la question. »*

7 Il ressort de l'ensemble de ces éléments, combinés avec les décisions ayant renvoyé les présentes questions préjudicielles, que le Conseil d'État estime que la Cour de justice de l'Union européenne se serait mépris en adoptant son arrêt Tele2 Sverige AB. En réalité, sous couvert d'un « dialogue des juges » le Conseil d'État vient ainsi notifier à la Cour de justice qu'il ne partage pas sa jurisprudence.

8 En l'espèce, pourtant, loin d'avoir « *inexactement pesé les différents éléments du débat* », la Cour de justice de l'Union européenne avait bien au contraire pris une décision soigneusement réfléchie et équilibrée.

9 En premier lieu, tant l'arrêt Tele2 Sverige AB que l'arrêt DRI de 2014 ont été adoptés par la Cour en formation de Grande Chambre, soit la formation la plus solennelle, disposant de la plus grande autorité dans l'interprétation du droit de l'Union européenne.

10 En deuxième lieu, dans l'arrêt Tele2, la Grande Chambre s'est sensiblement éloignée des conclusions de son propre avocat général, M. Henrik Saugmandsgaard Øe, qui souhaitait retenir une solution moins protectrice des libertés et droits fondamentaux des citoyens européens, montrant ainsi que ce n'est pas par mégarde ou par méconnaissance que cet arrêt était rendu. Au contraire, la Cour de justice a rendu sa décision en toute connaissance de cause.

11 Enfin, cet arrêt a été rendu dans un contexte particulièrement anxiogène, où l'Europe était en proie à une recrudescence d'attentats terroristes. Par la suite, loin d'avoir occulté les contraintes et réalités concrètes de la lutte contre le terrorisme et, plus largement, contre la criminalité, la Cour a soigneusement pris en compte les différentes composantes du débat et a assuré un parfait équilibre entre celles-ci.

12 La première question de l'affaire 511/18 et la première question de l'affaire 512/18 sont presque identiques et concernent les obligations imposées aux **opérateurs de télécommunications**. Elles seront traitées dans un premier temps (section 2).

13 La seconde question transmise dans l'affaire 512/18 concerne, en outre, les obligations imposées aux **hébergeurs**. Elle sera traitée dans un second temps (section 3 page 11).

2 La conservation généralisée imposée aux opérateurs

14 En substance, par deux questions, le Conseil d'État demande à la Cour de justice de définir les conditions, si elles existent, dans lesquelles le droit de l'Union permettrait

aux États membres d'imposer aux opérateurs de télécommunications la conservation des données de connexion de l'ensemble de leurs utilisateurs. Précisément, le Conseil d'État demande si l'une de ces conditions pourrait être :

— « *un contexte marqué par des menaces graves et persistantes pour la sécurité nationales, et en particulier le risque terroriste* » (première question de l'affaire C-511/18) ou :
— l'existence de « *garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion* » (première question de l'affaire C-512/18).

* § Le Conseil d'État laisse ainsi entendre que la Cour de justice devrait modifier sa jurisprudence, qui interdit sans exception les régimes de conservation généralisée. Ce faisant, le Conseil d'État se méprend : le droit de l'Union ne permet la conservation généralisée des données de connexion ni au regard de la sécurité nationale (section 2.1) ni au regard d'hypothétiques garanties et contrôles additionnels (section 2.2 page 8).

2.1 La sécurité nationale ne justifie pas l'obligation

15 Le Conseil d'État livre une interprétation erronée du droit de l'Union lorsqu'il considère que la lutte contre le terrorisme relève de la sécurité nationale (2.1.1) et que la sécurité nationale pourrait justifier à elle seule des mesures de surveillance mises en œuvre pour des finalités bien plus larges (2.1.2). Enfin, le Conseil d'État se fonde sur une mauvaise interprétation de la situation factuelle actuelle lorsqu'il considère que l'évolution du risque terroriste justifierait un changement du droit (2.1.3).

2.1.1 La lutte contre le terrorisme ne relève pas de la sécurité nationale

16 Dans sa question posée à la Cour, le Conseil d'État vise « *un contexte marqué par des menaces graves et persistantes pour la sécurité nationales, et en particulier le risque terroriste* », soulignant que la lutte contre le terrorisme entrerait dans le domaine de la sécurité nationale. Il n'en est rien.

17 Le domaine de la sécurité nationale est défini à l'article 4, §2, du Traité sur l'Union européenne (TUE) comme un domaine qui « reste de la seule responsabilité de chaque État membre ». Il s'agit donc d'une définition négative qui délimite ce domaine à toutes les **questions de sécurité à propos de laquelle l'Union n'est pas compétente pour légiférer**.

18 Or, depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, l'article 83, §1, du Traité sur le fonctionnement de l'Union européenne (TFUE) prévoit que « le Parlement européen et le Conseil, statuant par voie de directives conformément à la *procédure législative ordinaire*, peuvent établir des règles » dans les domaines suivants : « le *terrorisme*, la traite des êtres humains [...] ». À ce titre, l'Union a notamment adopté la directive 2017/541 « relative à la lutte contre le terrorisme » qui « énumère de manière exhaustive un certain nombre d'infractions graves, telles que les atteintes à la vie d'une

personne, en tant qu'actes intentionnels pouvant être qualifiés d'infractions terroristes » (considérant 8).

19 Ainsi, la lutte contre le terrorisme entre bel et bien dans les compétences législatives de l'Union. Elle ne relève pas « de la seule responsabilité de chaque État membre » et est dès lors exclue du domaine de la sécurité nationale.

20 Par ailleurs, afin d'identifier si une finalité poursuivie relève de la sécurité nationale, les dispositions du TUE et du TFUE se bornent à déterminer si l'Union est compétente ou non pour légiférer à ce sujet, sans s'attarder sur la façon dont cette finalité pourrait être poursuivie. Ainsi, il importe peu qu'une finalité soit poursuivie de façon *préventive*, par des services secrets cherchant à détecter des menaces, ou de façon *répressive*, par des juges et la police cherchant à identifier et punir un coupable.

21 À ce titre, la directive 2016/680 définit son champ d'application en visant indistinctement tout traitement de données personnelles réalisé « à des fins de *prévention et de détection* des infractions pénales, d'enquêtes et de *poursuites* en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la *sécurité publique* et la prévention de telles menaces » (article premier).

22 Dès lors, la prévention, la détection et la répression des infractions, notamment terroristes, entrent toutes dans la compétence législative de l'Union et sont, en conséquence, exclues du domaine de la sécurité nationale. Cette qualification empêche les États membres de bénéficier d'une quelconque *marge de manœuvre* dès qu'ils mettent en place des mesures poursuivant l'une de ces finalités. Ils doivent nécessairement respecter l'ensemble des garanties exigées par le droit de l'Union.

2.1.2 L'obligation s'apprécie au regard de toutes les finalités poursuivies

23 Le Conseil d'État demande si « *un contexte marqué par des menaces graves et persistantes pour la sécurité nationale* » est un élément qui permettrait aux États Membres d'imposer aux opérateurs une obligation de conservation de l'ensemble des données de connexion de leurs utilisateurs, et justifierait que la Cour modifie sa jurisprudence sur la base de ce seul critère.

24 En droit français, l'administration peut accéder aux données de connexions sur la base de nombreuses finalités (certaines sont citées ci-dessous). La sécurité nationale constitue seulement l'un de ces motifs qui, en pratique, est utilisé de façon minoritaire.

25 En effet, en 2015, dans son 23ème rapport d'activité, la Commission nationale de contrôle des interceptions de sécurité (CNCIS, l'autorité notifiée de la mise en place des techniques de renseignement jusqu'à 2015) précisait que, « entre le 1er janvier et le 30 avril 2015, [...] la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 48%, suivie de la prévention du terrorisme avec 38% [...] et de *la sécurité nationale avec 12%* » (au passage, on note une distinction claire entre terrorisme et sécurité nationale). Ces chiffres ne concernent que les interceptions de communications et non les accès aux données de connexion, pour lesquels aucun chiffre équivalent n'a

encore été publié. Il semble toutefois improbable que cette répartition entre les finalités soit sensiblement différente en matière d'accès aux données de connexion.

26 La proportionnalité des atteintes aux libertés fondamentales qu'engendre un régime de conservation généralisée doit être évaluée au regard de *l'ensemble des finalités* que ce régime permet de poursuivre, et non au regard d'une seule d'entre elles qui, en outre, est minoritaire.

27 Pour justifier ces atteintes, *toutes* ces finalités doivent « répondre à des *critères objectifs*, établissant un rapport entre les données à conserver et l'objectif poursuivi » et « s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné » (Tele2, § 110). De plus, en matière de lutte contre les infractions, « seule la lutte contre la *criminalité grave* est susceptible de justifier une telle mesure » (Tele2, § 102).

28 En pratique, l'administration française est notamment autorisée à accéder aux données de connexion obligatoirement conservées pour :

- la défense des « intérêts majeurs de la **politique étrangère** », ces intérêts étant discrétionnairement définis par le Gouvernement (code de la sécurité intérieure, ci-après « CSI », article L811-3, 2°) ;
- « l'exécution des engagement **européens et internationaux** de la France » (CSI, L811-3, 2°), notamment l'application des normes de l'Union européenne sur l'agriculture, la pêche, les transports, l'emploi, la culture ou le tourisme ainsi que les accords internationaux tels que l'accord de Paris de 2015 sur le climat ou la Convention de Genève de 1931 sur le droit de timbre en matière de chèque ;
- la défense des « intérêts **économiques, industriels et scientifiques** de la France » (CSI, L811-3, 3°), qui permet l'espionnage industriel et scientifique ;
- les prévention des « violences collectives de nature à porter gravement atteinte à la paix publique » (CSI, L811-3, 5°, c), couvrant notamment la lutte contre les **manifestations**, même non-violentes, n'ayant pas été déclarées ou ayant fait l'objet d'une déclaration incomplète (voir la décision DC 2015-713 du Conseil constitutionnel français qui, à son considérant 10, renvoie aux articles 431-1 à 431-10 du code pénal pour définir cette finalité, notamment celle prévue à l'article 431-9 du code pénal) ;
- « la prévention de la criminalité et de la délinquance organisée » (CSI, L811-3, 6°), notamment la lutte contre l'acquisition illicite de **stupéfiants**, même par un individu seul qui n'agit pas en groupe (voir la décision DC 2015-713 du Conseil constitutionnel français qui renvoie aux infractions listées à l'article 706-73 du code de procédure pénale pour définir cette finalité, notamment celle prévue à l'article 222-37 du code pénal) ;
- la lutte par la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI) contre les personnes échouant à **sécuriser leur accès à Internet** qui a permis le partage d'une œuvre protégé par le droit d'auteur (articles L34-1 du code des postes et des communications électroniques et L336-3 du code de la propriété intellectuelle).

29 **Aucune des ces finalités ne remplit les critères de proportionnalité** exigés par le droit de l'Union. Certaines ne sont limitées par aucun critère suffisamment objectif : politique étrangère, respect des engagements internationaux, intérêts économiques, industriels

et scientifiques. Certaines concernent la lutte contre des infractions qui ne peuvent pas être qualifiées de crimes graves : organisation de manifestation non déclarée, acquisition de stupéfiant à titre personnel et défaut de sécurisation de l'accès à Internet.

30 Dès lors, il parait cohérent et nécessaire que la Cour se prononce, au préalable, sur l'absence de proportionnalité des finalités déjà prévues en droit français, tant pour accéder que conserver les données de connexion. Ce n'est qu'après qu'elle pourra se pencher sur la question de savoir si d'autres motifs auraient pu justifier une conservation généralisée.

2.1.3 L'évolution du contexte ne justifie pas l'obligation

31 Le Conseil d'État vise « *un contexte marqué par des menaces graves et persistantes pour la sécurité nationales, et en particulier le risque terroriste* », soulignant un contexte qui aurait évolué depuis le jour où la Cour de justice a construit la jurisprudence qu'il remet en question. Or, si le contexte terroriste a évolué, ce n'est pas dans un sens appelant à affaiblir la protection des libertés fondamentales.

32 L'arrêt Tele2, qui qui interdit tout régime de conservation généralisée, a été rendu le 21 décembre 2016, dans un contexte bien plus anxiogène qu'aujourd'hui. L'arrêt a été rendu deux ans après les 17 morts des attentats des frères Kouachi (du 7 au 9 janvier 2015), un an après après les 130 morts des attentats de Paris (le 13 novembre 2015), neuf mois après les 32 morts de Bruxelles (le 22 mars 2016) et cinq mois après les 86 morts de Nice (le 14 juillet 2016). Ceci n'a pas empêché la Cour de justice de souligner explicitement dans sa décision que le terrorisme ne justifiait pas la conservation généralisée des données de connexion : « *si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte* » (§ 103).

33 Entre les périodes 2015-2016 et 2017-2018, le nombre de victimes du terrorisme dans l'Union européenne a presque été divisé par quatre [4]. Cette évolution est à attribuer à de nombreux facteurs complexes. Le gouvernement français pourrait être tenté d'attribuer cette évolution aux nouveaux pouvoirs que lui a conféré la loi renseignement du 24 juillet 2015, mais il ne pourra pas nier que l'année qui a suivi l'adoption de cette loi a été la plus meurtrière que la France ait connu depuis la guerre d'Algérie, et ce alors même que, du propre aveu du gouvernement, cette loi se contentait d'autoriser des mesures déjà mises en œuvres par les services de renseignement depuis plusieurs années.

34 Cette division par quatre du nombre de victime ne révèle pas un besoin d'aggraver les atteintes aux libertés fondamentales au nom de la lutte contre le terrorisme. Cette évo-

4. Depuis l'arrêt Tele2, deux attentats survenus dans l'Union européenne ont fait plus de dix victimes : 22 morts à la sortie d'un concert à Manchester (le 22 mai 2017) et 16 morts dans les rues de Barcelone (les 17 et 18 août 2017). À côté, 28 personnes de plus ont succombé à des attaques terroristes faisant moins de dix victimes (14 morts au Royaume-Unis les 22 mars, 3 juin et 18 juin 2017 ; 8 morts en France les 20 avril et 1er octobre 2017 et les 23 mars et 12 mai 2018 ; 1 mort en Allemagne le 28 juillet 2017 ; 2 morts en Finlande le 18 août 2017 ; 3 morts en Belgique le 29 mai 2018).

lution du risque terroriste ne justifie pas que la Cour de justice rende aujourd'hui une décision différente de celle rendue il y a deux ans. Au contraire.

2.2 Aucune garantie ni aucun contrôle ne peut justifier l'obligation

35 Le Conseil d'État demande à la Cour de justice de définir quelles « *garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion* » seraient à même de justifier des dispositions nationales imposant aux opérateurs de télécommunications de conserver les données de connexion de l'ensemble de leurs utilisateurs.

36 Alors que la Cour de justice a déjà affirmé dans l'arrêt Tele2, rendu en grande chambre, qu'aucune garantie ou contrôle ne permettait de justifier une telle conservation, le Conseil d'État lui demande de revoir sa position. Il lui demande notamment de chercher de nouvelles exigences plus strictes quant à l'accès et l'utilisation des données (en aval) qui pourraient en justifier la conservation généralisée (en amont).

37 En premier lieu, il convient de rappeler le contexte juridique dans lequel le Conseil d'État a transmis sa question préjudicielle. En effet, puisque le droit français ne respecte pas les exigences déjà imposées par le droit de l'Union en matière d'accès et d'utilisation des données de connexion, il semble inutile que la Cour de justice en cherche de nouvelles, plus strictes, qu'il ne respectera manifestement pas davantage (2.2.1).

38 Plus largement, au delà du seul cas français, il n'existe aucune garantie capable d'endiguer de façon réaliste les risques causés par une obligation de conserver les données de connexion de l'ensemble de la population, et ce alors même que cette conservation généralisée obligatoire n'est pas nécessaire à la poursuite des finalités avancées (2.2.2).

2.2.1 Le droit français ne respecte déjà pas le droit de l'Union

39 Le Conseil d'État évoque des « *garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion* ».

40 En matière de surveillance administrative, le droit français opère une distinction claire entre le recueil des données de connexion et leur utilisation ultérieure. Aucun de ces deux types de traitement n'est soumis à des garanties suffisantes ou à un contrôle effectif.

a. Le recueil des données de connexion n'est pas encadré par des garanties suffisantes

41 L'article 52, paragraphe 1, de la Charte prévoit que « *toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi* ». Cela implique notamment deux choses.

42 Premièrement, une disposition autorisant l'accès aux données de connexion par l'administration doit « prévoir des *règles claires* et précises indiquant en quelles circonstances

et sous quelles conditions » cette mesure est possible et « se fonder sur des critères objectifs pour définir [c]es circonstances et [c]es conditions » (Tele2, § 109 et § 119). Tel que démontré ci-avant, le droit français ne respecte pas cette garantie, puisqu'il permet l'accès aux données de connexion pour des finalités qu'il définit de façon particulièrement large et dont le champ est discrétionnairement défini par le gouvernement.

43 Secondement, une telle disposition est aussi disproportionnée si elle « ne prévoit aucun critère objectif permettant de *limiter le nombre de personnes* disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées » (Digital Rights Ireland, § 62). L'article L811-4 du CSI donne toute latitude au gouvernement pour désigner les services de l'administration, autres que les « services spécialisés de renseignement » définis par la loi, qui peuvent recourir aux techniques de renseignement, notamment pour recueillir des données de connexion auprès des opérateurs. Le droit français ne prévoit aucun critère objectif pour empêcher le gouvernement d'augmenter indéfiniment le nombre de ses agents autorisés à recourir à ces mesures.

44 En outre, l'article 47 de la Charte prévoit que « toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un *recours effectif* devant un tribunal ». Tel que l'explique La Quadrature du Net dans ses écritures (section 2), les recours prévus contre les techniques de collecte de renseignement, dont l'accès aux données de connexion fait partie, sont soit inexistants soit non-effectifs.

b. Le recueil des données de connexion n'est pas soumis à un contrôle effectif

45 L'article 8, paragraphe 3, de la Charte prévoit que « le respect [des règles sur la protection des données] est soumis au contrôle d'une autorité indépendante ». En matière de données de connexion, cela implique que « il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifié, subordonné à un *contrôle préalable* effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités » (Tele2, § 120).

46 Le recueil de données de connexion par les services de renseignement français est encadré par les dispositions du livre VIII du code de la sécurité intérieure.

47 L'article L821-2 du CSI prévoit que la demande d'accès est formulée par le ministre de la défense, de l'intérieur, de la justice ou de l'économie au Premier Ministre, au nom des agents de leurs services qui la réclament. L'article L821-3 prévoit que la commission nationale de contrôle des techniques de renseignement (CNCTR), qui est l'entité indépendante du gouvernement censée contrôler ces mesures, est uniquement notifiée de la demande d'autorisation adressée au Premier Ministre. Mais la CNCTR n'a aucun pouvoir pour s'y opposer. Elle peut uniquement indiquer au Premier Ministre qu'elle considère que la technique demandée serait illicite puis, si le Premier Ministre l'autorise toutefois, saisir le Conseil d'État pour s'opposer à la mesure. Sa saisine du Conseil d'État ne suspend pas la mise en œuvre de la mesure, la décision du Conseil d'État pouvant être rendu bien plus tard (la loi n'impose pas de délai fixe).

48 Ainsi, en pratique, aucune autorité indépendante n'a le pouvoir d'empêcher que des renseignement ne soient collectés en violation de la loi. Aucune « demande motivée » n'est jamais faite auprès de la CNCTR, qui est surtout spectatrice et ne peut prendre aucune

décision contraignante. Au mieux, la CNCTR peut intervenir une fois que l'atteinte à la protection de ces données a été réalisée, pour demander au Conseil d'État la suppression d'informations qui ont déjà pu être exploitées illégalement. L'action de la CNCTR **intervient systématiquement après la collecte** des données : il ne s'agit pas d'un contrôle préalable, ce qui oblige à constater, une fois encore, la contrariété du régime français aux garanties exigées par le droit de l'Union européenne.

c. L'utilisation ultérieure des données de connexion n'est soumise à aucune garantie ni contrôle

49 La Cour de justice reconnaît qu'est contraire à la Charte une mesure de surveillance qui « *ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure* » à ce qui est strictement nécessaire (Digital Rights Ireland, § 60).

50 En droit français, le CSI n'encadre que les techniques de collecte, de transcription et d'extraction des données, mais pas l'utilisation qui est faite des informations ainsi réunies. Autrement dit, en droit français, une fois que les données ont été collectées, transcrites et extraites, pour être mises en forme de façon utilisable par les services (fiche, dossier), *aucun cadre juridique ne limite l'utilisation ultérieure* qui peut en être faite.

51 Tout au plus, l'article L822-3 prévoit que, s'agissant des données collectées pour les finalités prévues à l'article L811-3, « *les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités* ». Mais cette disposition ne limite que la conservation des informations et, en aucun cas, leur utilisation. Par exemple, elle n'empêche pas qu'une fiche valablement conservées pendant un an à des fins de surveillance économique soit, pendant cette même durée, aussi utilisée pour des finalités politiques étrangères à celle-ci.

52 De même, aucune trace n'est gardée des accès réalisés par l'administration aux informations qu'elle a réunies. Si l'article L822-1 du CSI prévoit que « le Premier ministre organise la traçabilité de l'exécution des techniques autorisées en application du » livre VIII du CSI, cette traçabilité ne concerne que la réalisation des « techniques de recueil de renseignement ») et non *l'utilisation* des renseignements collectés.

53 Enfin, la CNCTR a certes accès aux renseignements, mais la loi ne lui donne *aucun pouvoir de contrôle* sur l'utilisation qui en est faite par les services, ne serait-ce qu'a posteriori. Si le CSI ouvre une voie de recours devant le Conseil d'État contre la mise en œuvre de technique de recueil de renseignement, il ne prévoit rien pour contester en justice la façon dont les renseignements collectés sont utilisés.

2.2.2 L'obligation n'est pas nécessaire

54 L'écart entre ce que permet le droit français et ce qu'exige le droit de l'Union est si grand qu'il serait irréaliste d'espérer poser des garanties et des contrôles à même de justifier la conservation généralisée des données de connexion. De nombreux États membres ne respecteront pas ces garanties et ces contrôles, de même qu'ils ont refusé sans nuance depuis quatre ans de respecter l'interdiction de conservation généralisée dégagée de la Charte par la Cour de justice (voir le rapport de septembre 2017 réalisé

par Privacy International sur le défaut de transposition nationale de l'arrêt Tele2 dans l'Union européenne : `https://privacyinternational.org/advocacy-briefing/735/report-national-data-retention-laws-cjeus-tele-2watson-judgment`).

55 Cette tentative hasardeuse serait d'autant moins justifiée que la nécessité d'une telle conservation généralisée s'efface d'année en année, devenant aujourd'hui automatiquement disproportionnée aux finalités qu'elle poursuit, peu importe les garanties qui l'encadrent.

56 En effet, le gouvernement français a systématiquement échoué à présenter des éléments concrets et chiffrés au soutien de la nécessité de son régime de conservation généralisé. Tout au plus, il a mis en avant quelques exemples de procédures ayant eu recours à des données de connexion, mais n'a jamais expliqué matériellement en quoi l'accès à ces données aurait été décisif pour le succès d'une procédure, et cela de façon général, au-delà de quelques exemples choisis et peu représentatifs.

57 Ce débat factuel serait d'autant plus indispensable que les usages des communications électroniques ont largement évolué ces dernières années. Les services Web (messageries instantanées, email, réseaux sociaux) *collectent et conservent volontairement* de plus en plus de données pour leurs propres besoins, notamment techniques, tel qu'exposé dans la prochaine section des présentes écritures. Le gouvernement n'a jamais su démontrer en quoi ces données ne seraient pas suffisantes pour poursuivre les objectifs qu'il se donne.

58 De plus, le droit aussi est en train d'évoluer : la Commission européenne a proposé le 17 avril 2018 un nouveau règlement « relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale » (parfois appelé « E-Evidence »). Cette proposition prévoit notamment que les autorités publiques pourront émettre des *injonctions de conservation* aux prestataires techniques afin que ceux-ci conservent des données de connexion pour une durée allant jusqu'à 60 jours, empêchant « l'effacement, la suppression ou la modification des données concernées » (considérant 36). Il faut souligner que cette proposition répond au point 108 de l'arrêt Tele2 où la Cour de justice reconnaissait comme conforme à la Charte les mesures de conservation ciblée.

59 Ces évolutions pratiques et législatives rendent encore moins nécessaires, et donc encore moins proportionnées, les obligations de conservation généralisée par rapport à ce qu'elles étaient lorsque que la Cour de justice les a déclarées contraire au droit de l'Union.

3 La conservation généralisée imposée aux hébergeurs

60 En substance, dans sa question visant les hébergeurs (il s'agit de la seconde question transmise dans l'affaire C-512/18), le Conseil d'État demande à la Cour de justice si le droit de l'Union est compatible avec des dispositions qui, telles que celles prévues en droit français, imposent aux hébergeurs de conserver pendant un an les données de connexion de l'ensemble de leurs utilisateurs ayant contribué à la publication de contenus.

61 Dans la décision par laquelle il transmet cette question, le Conseil d'État considère que

la directive 2002/58 ne permet pas d'y répondre. Le Conseil d'État déduit cette impossibilité du fait que cette directive ne serait pas applicable aux hébergeurs. Il en conclut que la proportionnalité d'une obligation de conservation généralisée peut être appréciée différemment selon qu'elle s'impose à des hébergeurs ou à des opérateurs de télécommunications. Cette interprétation du droit de l'Union est erronée (section 3.1).

62 De façon générale, en matière de conservation des données, il n'existe aucune raison matérielle ou juridique de prévoir des obligations plus lourdes pour les hébergeurs que pour les opérateurs de télécommunications, celles-ci étant chaque fois contraire au droit de l'Union (section 3.2 page suivante).

3.1 La directive 2002/58 s'applique aux hébergeurs

63 Dans sa décision, le Conseil d'État affirme que la disposition française « *qui impose une obligation de détention et de conservation des seules données relatives à la création de contenu, n'entre pas dans le champ d'application de la directive du 12 juillet 2002, clairement réservé, aux terme de son article 3, paragraphe 1,* "au traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté*"* ».

64 Ainsi, le Conseil d'État formule sa question préjudicielle au regard de directive 2000/31 (qui décrit explicitement l'activité d'hébergement Web, à son article 14) et non pas de la directive 2002/58 (que le Conseil d'État ne considère pas encadrer l'activité des hébergeurs).

65 Pourtant, la Cour de justice a déjà jugé que « *la protection de la confidentialité des communications électroniques et des* ***données relatives au trafic*** *y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par* ***toutes les personnes autres que les utilisateurs****, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques* » (Tele2, § 77). Le champ de la directive dépend donc de la nature des données traitées et non de la personne qui les traite, dans la mesure où cette personne n'est pas l'utilisateur.

66 À ce titre, la Cour de justice a précisé que les données de trafic « *permettent de retrouver et d'identifier* la source d'une communication et la destination de celle-ci, de déterminer *la date, l'heure, la durée et le type* d'une communication [...]. Au nombre de ces données figurent, notamment, **le nom et l'adresse** de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une *adresse IP* pour les services Internet » (Tele2, § 98).

67 En France, l'article 6, paragraphe 8, de la LCEN prévoit que les hébergeurs « détiennent et conservent 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 ».

68 L'article 1 du décret 2011-219 du 25 février 2011 précise que ces données sont notamment :
- « l'identifiant de la connexion à l'origine de la communication », ce qui recoupe au moins *l'adresse IP* ;

— « l'identifiant attribué par le système d'information au contenu » ;
— « les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus » et « la nature de l'opération » (ajout, suppression ou modification du contenu), ce qui recoupe le *type de la communication réalisée* ;
— « les *date et heure* de l'opération » et de la communication qui l'a permise ;
— « les *nom et prénom* », « les adresses postales associées » et « les adresses de courrier électronique » fournies aux moment de la création d'un compte.

69 Il en résulte que la loi française impose aux hébergeurs de conserver des données que le droit de l'Union qualifie de « données de trafic ». Le traitement de telles données déterminant le champ d'application de la directive 2002/58, ce texte est donc *applicable aux hébergeurs* qui conservent ces données.

70 D'ailleurs, les dispositions de la directive 2002/58 encadrant l'utilisation de *cookies* et d'autres traceurs techniques deviendraient largement ineffectives si cette directive n'était pas applicable aux hébergeurs et aux sites Web, alors que c'est principalement pour encadrer l'activité de ces acteurs-ci que ces dispositions ont été adoptées par l'Union européenne.

71 En conclusion, contrairement à ce que le Conseil d'État l'invite à faire, la Cour de justice peut et doit évaluer la proportionnalité d'une obligation de conservation de données de connexion imposée aux hébergeurs de la même façon qu'elle a évaluée cette obligation lorsqu'elle est imposée aux opérateurs : c'est-à-dire au regard des garanties exigées par la directive 2002/58 et, de là, par la Charte.

3.2 L'obligation imposée aux hébergeurs est tout autant disproportionnée que celle imposée aux opérateurs

72 Le raisonnement qui a conduit la Cour de justice à déclarer l'obligation imposée aux opérateurs contraire à la Charte doit conduire à la même conclusion s'agissant de l'obligation imposée aux hébergeurs : la Cour a déjà établi une telle symétrie sur des sujets connexes (3.2.1) ; la conservation de données de connexion par les hébergeurs cause des ingérences équivalentes (3.2.2) ou plus graves (3.2.3) que celle imposée aux opérateurs ; cette obligation de conservation n'est pas nécessaire (3.2.4).

3.2.1 Une symétrie déjà reconnue en matière de surveillance active

73 En matière de surveillance active, la Cour de justice a déjà aligné le régime des hébergeurs sur celui des opérateurs de télécommunications. Son arrêt Scarlet sur les fournisseurs d'accès à Internet (FAI) et son arrêt Netlog sur les hébergeurs reconnaissent chacun la même chose : imposer à l'un de ces acteurs une « surveillance active de l'ensemble des données concernant tous ses clients [...] entraînerait une atteinte caractérisée à la liberté d'entreprise », au « droit à la protection des données à caractère personnel et [à] la liberté de recevoir ou de communiquer des informations » et ne serait pas compatible avec ces libertés fondamentales telles que protégées par l'Union européenne (Scarlet c. SABAM,

CJUE, 3ème ch., 24 novembre 2011, C-70/10, paragraphes 40, 48 et 53 ; SABAM c. Netlog, CJUE, 3ème ch., 16 février 2012, C-360/10, paragraphes 38, 46 et 51).

74 La parfaite symétrie établie par la Cour entre les FAI et les hébergeurs en matière de surveillance active doit se prolonger en matière de surveillance passive, c'est à dire en matière de conservation des données de connexion.

3.2.2 Une ingérence tout aussi importante s'agissant de l'adresse IP

75 La Cour de justice a déclaré contraire à la Charte toute obligation de conservation généralisée des données de connexion par les FAI au motif que, « prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » et que, « en particulier, ces données fournissent les moyens d'établir [...] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications ». L'ampleur de ces ingérences a été reconnue comme disproportionnée par rapport aux buts poursuivis.

76 L'ingérence permise par l'obligation imposée aux FAI résulte du fait que ces FAI conservent des informations permettant d'associer le nom d'une personne à l'adresse IP qu'elle a utilisée pour envoyer certaines informations à un moment donné. Or, dans la plupart des cas, l'obligation de conservation généralisée imposée aux hébergeurs produit exactement les mêmes effets : les informations conservées par les hébergeurs permettent aussi d'associer une adresse IP donnée au nom de la personne qui l'a utilisée.

77 Typiquement, l'hébergeur d'un réseau social connaît l'adresse IP utilisée par chacun des ses utilisateurs, identifiés par un pseudonyme unique. Souvent, ce pseudonyme peut être recoupé avec d'autres informations (amis, lieux, photo, activités) afin de retrouver l'identité de la personne. Dans d'autre cas, le pseudonyme n'est pas différent du nom officiel de la personne. Ainsi, en 2016, le CNIL expliquait que 43% des utilisateurs français de réseaux sociaux n'utilisaient jamais de pseudonyme pour s'y inscrire (Baromètre générique sur les pratiques numériques et la maîtrise des données personnelles. Synthèse de résultats – Vague 2016, 19 septembre 2016, CNIL `https://linc.cnil.fr/sites/default/files/atoms/files/synthese_cnil_barometre_generique_2016.pdf`).

3.2.3 Une ingérence plus importante s'agissant des autres informations

78 Contrairement aux FAI, les informations conservées par les hébergeurs révèlent bien plus d'informations que la seule identité de la personne ayant utilisée une adresse IP à un moment donnée. Savoir qu'une personne a contribué à tel contenu, à tel moment, sur telle page, en relation avec telles autres personnes ou tels groupes et à telle fréquence permet directement d'établir un profil sur les personnes concernées. C'est précisément le fonctionnement des grands réseaux sociaux qui, déjà, établissent des profils publicitaires particulièrement précis sur leurs utilisateurs à partir de ces mêmes informations

(d'ailleurs, la conformité de ces activités au droit de l'Union est aujourd'hui largement contestée devant les autorités de protection des données).

79 Les informations conservées par les FAI ne permettent pas d'établir de profils aussi précis : pour produire un profil, ces informations doivent être recoupées avec d'autres informations détenues par d'autres acteurs, notamment des hébergeurs. La Cour de justice a pourtant reconnu que la conservation généralisée imposée aux FAI était disproportionnée. Il en résulte que la proportionnalité des obligations imposées aux hébergeurs, dont les conséquences sont bien plus graves et directes, doit être évaluée au moins aussi fermement.

80 Enfin, l'importance de l'ingérence permise est d'autant plus grande que certains hébergeurs détiennent, à eux seuls, des informations extrêmement denses sur une très large partie de la population. Le cas le plus révélateur est celui de Facebook qui, parmi les 512 millions de personnes vivant en Europe, est utilisé en 2018 au moins une fois par mois par 376 millions de personnes (voir `https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/`).

81 En conclusion, comparées aux obligations de conservation imposées aux FAI, qui poursuivent les mêmes finalités, les conséquences pour la vie privée et la protection des données personnelles de la population sont équivalentes (s'agissant de l'identification de la personne utilisant une adresse IP) ou plus graves (s'agissant de retracer les activités et modes de vie) lorsque les hébergeurs sont obligés de conserver les données de connexion de l'ensemble des personnes ayant contribué aux contenus qu'ils diffusent. La Cour de justice ne peut que déclarer cette obligation contraire aux exigences de proportionnalité prévues par la Charte.

3.2.4 L'obligation n'est pas nécessaire

82 Le règlement général sur la protection des données (RGPD) et la directive 2002/58 autorisent les hébergeurs à conserver des données personnelles pour diverses finalités : notamment, des finalités de facturation et de sécurité ou, avec le consentement des utilisateurs, des finalités publicitaires. Ainsi, la seule finalité de sécurité permet aux hébergeurs de conserver pendant une durée non négligeable les données de connexion (adresse IP, date et nature de la communication) concernant l'ensemble des utilisateurs contribuant aux contenus publiés en ligne, ne serait-ce que pour se prémunir d'attaques par déni de service ou de publications commerciales automatisées non-souhaitées.

83 Les hébergeurs conservent donc, pour des raisons diverses et indépendantes d'une obligation légale de conservation généralisée, un certain nombre de données, y compris des données de trafic. Corrélées entre elles, ces données fournissent des informations d'une précision incroyable sur les utilisateurs. Encore une fois, les autorités françaises échouent à démontrer en quoi ces informations seraient structurellement insuffisantes au point de rendre nécessaire une conservation obligatoire par les hébergeurs.

84 Enfin, tel qu'exposé au sujet des opérateurs de télécommunication, le futur règlement E-Evidence prévoit déjà toutes les mesures pour compenser les quelques cas où la conservation spontanée de la part des hébergeurs ne semblerait pas suffisante : des *injonctions de conservation* les obligeant à conserver les données de connexion pour une durée allant

jusqu'à 60 jours, empêchant « *l'effacement, la suppression ou la modification des données concernées* ».

85 En conclusion, obliger les hébergeurs à conserver des données de connexion relatives à l'ensemble des personnes ayant contribué aux contenus qu'ils diffusent n'est nécessaire et proportionné à la poursuite d'aucune finalité. Toute finalité peut être efficacement poursuivie par des mesures déjà mises en œuvre spontanément et causant une ingérence plus faible dans les libertés fondamentales de la population.