Conseil d'État
Section du contentieux
10e chambre
N° 393099

Observations complémentaires sur l'arrêt *Tele2*

PRODUIT PAR

1. **French Data Network (Réseau de données français)**, dit FDN
   Association régie par la loi du 1er juillet 1901 dont le siège social est situé au 16 rue de Cachy à Amiens (80090), enregistrée en préfecture de la Somme sous le numéro W751107563, opérateur déclaré auprès de l'ARCEP sous la référence 07/1149, prise en la personne de son président M. Fabien Sirjean, dûment habilité à agir en justice ;
   Tél. : 06 36 18 91 00
   Mail : contact@fdn.fr
2. **La Quadrature du Net**
   Association régie par la loi du 1er juillet 1901 dont le siège social est situé au 60 rue des Orteaux à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de son président M. Philippe Aigrain, dûment habilité à agir en justice ;
   Tél. : 06 73 60 88 43
   Mail : contact@laquadrature.net
3. **La Fédération des fournisseurs d'accès à Internet associatifs**, dite FFDN
   Association régie par la loi du 1er juillet 1901 dont le siège social est situé au 16 rue de Cachy à Amiens (80090), enregistrée en préfecture de la Somme sous le numéro W751210904, regroupant 27 fournisseurs d'accès associatifs français, déclarés auprès de l'ARCEP, et un fournisseur d'accès associatif belge déclaré auprès du régulateur, prise en la personne de son président M. Benjamin Bayart, dûment habilité à agir en justice.
   Tél. : 06 60 24 24 94
   Mail : contact@ffdn.org

CONTRE

Le refus implicite du Gouvernement d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, *JORF n° 50 du 1er mars 2011, p. 3643.*

TABLE DES MATIÈRES

I. FAITS ET PROCÉDURE

1 Le 6 mai 2015, les associations French Data Network (FDN), La Quadrature du Net, ainsi que la Fédération des fournisseurs d'accès à Internet associatifs (Fédération FDN) ont demandé au Gouvernement d'abroger l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et le décret n° 2011-219 du 25 février 2011 pris en application de la loi n° 2004-575 du 21 juin 2004 (LCEN). Ces dispositions règlementaires précisent les données de connexion devant être détenues ou conservées en application des dispositions législatives des articles L. 34-1 CPCE et 6, II, LCEN. D'après les termes de la demande d'abrogation des associations requérantes, ces dispositions instituent deux régimes de conservation généralisée et indifférenciée de données de connexion, contraires à l'article 15, paragraphe 1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (la Charte).

2 Le 6 juillet 2015, le Gouvernement a tacitement refusé d'abroger ces dispositions, alors même qu'un double changement de circonstances l'exigeait. [1]

3 Le 1er septembre 2015, les associations ont introduit un recours en excès de pouvoir contre ce refus tacite d'abrogation, complété par le dépôt d'un mémoire ampliatif produit le 27 novembre 2015. Le 8 février 2016, le Centre pour la démocratie et la technologie (« CDT ») et Privacy International ont formulé une intervention. En réponse au mémoire en défense du 20 juin 2016 déposé par le ministre de la Justice, garde des sceaux, les associations requérantes ont versé aux débats des observations en réplique par mémoire du 22 juillet 2016.

4 Les associations requérantes persistent et réitèrent l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures. Par la production des présentes observations complémentaires, elles entendent tirer les conséquences, dans la présente instance, de l'arrêt de la grande chambre de la Cour de justice du 21 décembre 2016 (CJUE, gde ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15), lequel confirme amplement le bien-fondé de la demande d'abrogation des dispositions litigieuses adressée au Gouvernement.

1. Voir la section 2 page 4 du mémoire ampliatif du 27 novembre 2015.

II. DISCUSSION

5 Après avoir rappelé que les dispositions litigieuses relèvent du champ d'application de l'article 15 de la directive 2002/58 (section 1), les associations requérantes entendent démontrer en quoi leur demande d'abrogation est fondée à plusieurs titres et notamment en raison, d'abord, de l'ingérence particulièrement grave que cause le droit français en matière de conservation des données de connexion (section 2 page 5) ; une ingérence d'une telle gravité ne pouvant pas être justifiée par la poursuite d'objectifs aussi larges ou indéfinis que ceux du droit français (section 3 page 8).

6 Ensuite, les associations requérantes insistent sur la motivation dépourvue de toute ambiguïté de la grande chambre de la Cour de justice. Celle-ci pose, très clairement, les exigences du strict nécessaire pour toutes mesures de conservation des données de connexion relevant de la directive 2002/58 — exigences que les régimes français de conservation généralisée ne respectent pas (section 4 page 11).

1. Sur le champ d'application de la directive 2002/58

7 **En droit,** il est indéniable que toute mesure législative visée à l'article 15 de la directive 2002/58 relève du champ d'application de cette directive. Cela concerne explicitement les mesures qui imposent aux fournisseurs de services de communications électroniques la conservation de données de trafic ou de localisation. Comme l'énonce la Cour de justice, toute interprétation contraire priverait d'effet utile l'article 15 de la directive 2002/58 (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, points 73). Relèvent également du champ d'application de la directive 2002/58, tel qu'il ressort de l'articulation de ses articles 3 et 15 : (i) des mesures imposant à ces fournisseurs le traitement de données à caractère personnel, et (ii) des mesures portant sur l'accès des autorités nationales aux données conservées (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, points 75 et 76 notamment).

8 Plus globalement, l'article 15 de la directive 2002/58 s'applique à toute mesure imposant à toute autre personne que l'utilisateur la conservation de

« données afférentes aux communications électroniques » et limitant de ce fait la confidentialité des communications protégée par l'article 5.

9 Comme le relève la grande chambre dans son arrêt *Tele2* :

> « En effet, 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. Comme le confirme le considérant 21 de cette directive, celle-ci vise à **empêcher « tout accès »** non autorisé aux communications, **y compris à « toute donnée afférente à ces communications », afin de protéger la confidentialité des communications électroniques**. »
>
> (point 77)
>
> [...]
>
> « Le principe de confidentialité des communications instauré par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, paragraphe 1, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, paragraphe 1, de cette directive et le stockage technique nécessaire à l'acheminement d'une communication (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 47). »
>
> (point 85)

10 En résumé, il ressort de l'interprétation faite par la Cour de justice de l'article 15 de la directive 2002/58 (lu en combinaison avec les articles 3 et 5 et à la lumière du considérant 21), que celui-ci s'applique à des mesures :

- Impliquant le traitement de données personnelles par les fournisseurs de services de communications électroniques, ou
- Imposant, à toute personne autre que l'utilisateur, la conservation de toute donnée afférente à des communications électroniques, ou
- Permettant, à toute personne autre que l'utilisateur, l'accès à de telles données.

11 **En l'espèce,** les dispositions dont l'abrogation a été demandée établissent une liste de données (couramment dites « données de connexion » [2]) qui doivent être traitées ou conservées [3]. Ces données de connexion se rapportent

2. au sens du chapitre I[er] du titre V du livre VIII du code de la sécurité intérieure

3. Sur la notion de « traitées ou conservées » voir notamment l'article L. 851-1 du code de la sécurité intérieure qui dispose que « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux*

non seulement à des « données relatives au trafic » [4] mais aussi aux « données de nature à permettre l'identification de quiconque a contribué » à un contenu en ligne. [5] Ces données constituent toutes, du point de vue de l'utilisateur, des données personnelles afférentes à ses communications.

12 D'une part, l'article R. 10-13, s'applique aux opérateurs (fournisseurs de réseaux ou de services de communications électroniques) et concerne certaines données de trafic et de localisation. Il résulte de l'application de l'article L. 34-1, III, qui impose notamment aux fournisseurs d'accès la conservation de données de trafic et de localisation. Cette disposition n'impose pas aux fournisseurs d'accès de détenir des données qu'ils ne traiteraient pas lors de l'acheminement des communications électroniques ou en vue de leur facturation.

13 D'autre part, le décret n° 2011-219 s'applique aux personnes mentionnées à l'article 6, I, 1 et 2 (c'est-à-dire les fournisseurs d'accès et les hébergeurs) et concerne des données identifiantes, y compris des données relatives au trafic (par exemple, l'identifiant de la connexion à l'origine de la communication) ainsi que d'autres données afférentes aux communications (par exemple, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus).

14 Le décret n° 2011-219 résulte de l'application de l'article 6, II, LCEN. À l'inverse de l'article L. 34-1 CPCE ; l'article 6, II, LCEN impose à la fois de détenir et de conserver des données afférentes aux communications électroniques, de telle sorte qu'il n'impose non seulement aux fournisseurs d'accès de *conserver* des données qu'ils traiteraient pour l'acheminement du trafic ou la facturation, mais également de *détenir* et donc de traiter des données supplémentaires. De plus, il impose aux hébergeurs une obligation de détention et de conservation de données afférentes aux communications électroniques.

15 Il résulte de ce qui précède que les régimes français de conservation de données de trafic, de localisation et d'autres données afférentes aux communications électroniques imposent la détention et/ou la conservation d'un ensemble de « données de connexion » plus large que le régime suédois en cause dans l'affaire *Tele2* (v. tableau comparatif en annexe), et ce pour une durée d'un an, soit deux fois supérieure à la durée du cas d'espèce dans l'affaire citée.

16 Il n'est pas contesté que toutes ces données doivent être considérées comme des données à caractère personnel. Dès lors, les dispositions litigieuses

---

1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents **traités ou conservés** *par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.* [...] »

4. au sens de l'article L. 32 18° CPCE
5. au sens de l'article 6, II, LCEN

imposant leur détention et/ou leur conservation impliquent nécessairement le traitement de données à caractère personnel et ce, que la personne concernée ait pu donner son consentement ou non.

17 Enfin, ces données se rapportent toutes à des communications du point de vue de l'utilisateur. Par conséquent, ces dispositions limitent toutes la confidentialité des communications électroniques.

18 En conclusion, il ne peut être contesté que les dispositions litigieuses impliquent la détention et/ou la conservation de données de trafic, de localisation ainsi que d'autres données afférentes à des communications électroniques, à l'insu des utilisateurs de services de communications électroniques et de services de communication au public en ligne.

19 **En conséquence,** les dispositions règlementaires dont l'abrogation est demandée, ainsi que les dispositions législatives sur lesquelles elles se basent, relèvent du champ d'application de la directive 2002/58.

20 Partant, les dispositions litigieuses doivent être compatibles avec cette directive, lue à la lumière des articles 7, 8, 11 et 52 de la Charte.[6] Or, les dispositions litigieuses — à l'instar des règlementations suèdoise, anglaise ou de la directive 2006/24 — sont incompatibles avec le respect des droits et libertés fondamentaux.

2. Sur la gravité et l'ampleur de l'atteinte aux droits fondamentaux causée par les dispositions litigieuses

21 Les dispositions de l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et du décret n° 2011-219 du 25 février 2011 pris en application de la loi n° 2004-575 du 21 juin 2004 (LCEN) causent une ingérence particulièrement grave et d'une vaste ampleur dans les droits et libertés des utilisateurs de services de communication au public en ligne et abonnés de services de communications électroniques, garantis par les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne.

22 **En droit,** l'obligation de conserver des données de connexion aux fins de les rendre, le cas échéant, accessibles aux autorités nationales, soulève des questions relatives non seulement aux droits au respect de la vie privée et à la protection des données personnelles garantis aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (la Charte),[7] mais également de la liberté d'expression garantie à l'article 11 de la Charte (ainsi que le rappelle la grande chambre de la Cour de justice aux points 93

6. Voir à ce sujet le mémoire complémentaire sur l'applicabilité de la Charte des droits fondamentaux de l'UE produit par les associations requérantes le 17 mai 2016.

7. Voir la section 1 page 7 du mémoire ampliatif du 27 novembre 2015.

et 101 de l'arrêt précité) [8].

23 Concernant le droit au respect de la vie privée et à la protection des données personnelles, ainsi que le relevait l'avocat général M. Saugmandsgaard Øe au point 254 de ses conclusions dans l'affaire *Tele2*, « une obligation générale de conservation de données permet des ingérences aussi graves que des mesures de surveillance ciblées, en ce compris celles interceptant le contenu des communications effectuées. » Il conclut que « les **risques liés à l'accès aux données** relatives aux communications (ou « métadonnées ») **peuvent être équivalents, voire supérieurs à ceux résultant de l'accès au contenu** de ces communications ».

24 L'avocat général M. Saugmandsgaard Øe ajoute, exemples et études à l'appui [9], que « les "métadonnées" permettent un catalogage presque instantané d'une population dans son entièreté, ce que ne permet pas le contenu des communications » (point 259, *Conclusions de l'avocat général M. Henrik Saugmandsgaard Øe*, 19 juill. 2016, C-203/15, C-698/15).

25 La Cour conclut à nouveau (cf. CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12) que l'ingérence que constitue la conservation généralisée des données de connexion est particulièrement grave et d'une vaste ampleur (en se référant expressément aux conclusions de l'avocat général qui viennent d'être soulignées) :

> « 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 (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 27). En particulier, ces données fournissent les moyens d'établir, *ainsi que l'a relevé M.*

8. Voir également la section 2 page 4 du mémoire en réplique du 22 juillet 2016 ainsi que la fin de la section 1.1 page 9 du mémoire ampliatif du 27 novembre 2015 sur l'entrave à la liberté de communication.

9. *Conclusions de l'avocat général M. Henrik Saugmandsgaard Øe*, 19 juill. 2016, C-203/15, C-698/15 :

> *Supposons, en premier lieu, qu'une personne ayant accès aux données conservées ait l'intention d'identifier, au sein de la population de l'État membre, tous les individus atteints de troubles d'ordre psychologique. L'analyse, à cette fin, du contenu de l'ensemble des communications réalisées sur le territoire national exigerait des ressources considérables. En revanche, l'exploitation des bases de données relatives aux communications permettrait d'identifier instantanément tous les individus ayant contacté un psychologue au cours de la période de conservation des données (83). J'ajoute que cette technique pourrait être étendue à chacune des spécialités médicales enregistrées dans un État membre (84).*
>
> *Supposons, en second lieu, que cette même personne souhaite identifier les individus opposés à la politique du gouvernement en place. À nouveau, l'analyse, à cette fin, du contenu des communications exigerait des ressources considérables. En revanche, l'exploitation des données relatives aux communications permettrait d'identifier tous les individus inscrits à des listes de distribution de courriels critiquant la politique du gouvernement. En outre, ces données permettraient également d'identifier les individus participant à toute manifestation publique d'opposition au gouvernement (85).* (points 256 et 257)

l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions [précités], 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'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte **s'avère d'une vaste ampleur** et doit être considérée comme **particulièrement grave**. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37). »

(points 99 et 100 de l'arrêt *Tele2*)

26 **En l'espèce,** l'ingérence constituée par les dispositions françaises imposant la conservation des données de connexion est encore plus grande et plus vaste que celle constituée par la directive 2006/24 [10] ou que celle constituée par le droit suédois [11] et, au moins équivalente à celle constituée par le droit anglais (tous deux en cause dans l'affaire *Tele2*) [12], en raison du champ plus large des données conservées, du champ plus large des personnes soumises à l'obligation de conservation et en raison, enfin, de la durée plus longue de conservation des données (cf. ¶ 15 page 4).

27 En effet, premièrement, le droit français impose la conservation des données à un plus grand nombre d'intermédiaires techniques, de telle sorte que cette conservation concerne un plus grand nombre d'utilisateurs. Par exemple, l'utilisateur d'un service de communication au public en ligne soumis au droit français verra ses données conservées par le prestataire de ce service (l'hébergeur) même s'il n'est pas abonné à un fournisseur d'accès soumis au droit français.

28 Deuxièmement, le droit français n'impose pas seulement aux fournisseurs d'accès de *conserver* des données qu'ils traiteraient pour l'acheminement du trafic ou la facturation, puisque le droit français impose également aux fournisseurs d'accès de *détenir* des données afférentes aux communications — dont certaines données inutiles à l'acheminement ou à la facturation qu'ils ne détiendraient pas en l'absence de cette obligation légale. C'est par exemple le cas de l'identifiant du terminal utilisé pour la connexion qui est inutile à l'acheminement ADSL.

10. Voir, notamment, la section 1.2 page 9 du mémoire ampliatif du 27 novembre 2015.

11. Voir le tableau comparatif en annexe des présentes observations.

12. Pour une énumération des données concernées dans les cas suédois et anglais, voir respectivement les points 17 et 18 ainsi que 31 de l'arrêt *Tele2* (mis en évidence en partie par le tableau comparatif joint en annexe des présentes). Dans le cas suédois, les données concernées se limitent à celles visées par la directive 2006/24. Dans le cas britannique, il s'agit de l'ensemble des données relatives au trafic à l'utilisation d'un service de télécommunication ainsi que des données détenues ou obtenues par des personnes fournissant un service de télécommunications en relation avec une personne utilisant un tel service.

29 **En conséquence,** il ne saurait être contesté que la conservation des données de connexion prévue en droit français cause une ingérence particulièrement grave et d'une vaste ampleur dans les droits et libertés des utilisateurs de services de communication au public en ligne et abonnés de services de communications électroniques.

3. Sur l'objectif susceptible de justifier la conservation des données

30 **En premier lieu**, les dispositions de l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et du décret n° 2011-219 du 25 février 2011 pris en application de la loi n° 2004-575 du 21 juin 2004 (LCEN) méconnaissent les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne en ce qu'elles ne limitent nullement la collecte et/ou la conservation des données de connexion à la poursuite d'objectifs susceptibles de justifier le caractère particulièrement grave et de vaste ampleur de l'ingérence qu'elles causent. [13]

31 **En droit,** les mesures qui relèvent du champ d'application de l'article 15 de la directive 2002/58 peuvent se justifier strictement par la poursuite d'un objectif d'intérêt général figurant à cet article. En effet, l'énumération des objectifs qui y figure revêt un caractère exhaustif (point 90 de l'arrêt *Tele2*). Ces objectifs sont :

- la sauvegarde de la sécurité nationale (ou la « sûreté de l'État »), la défense et la sécurité publique ;
- la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ;
- les objectifs visés à l'article 13, paragraphe 1, de la directive 95/46, à savoir ceux mentionnés précédemment ainsi que :

  d) la prévention, la recherche, la détection et la poursuite [...] de manquements à la déontologie dans le cas des professions réglementées ;

  e) la poursuite d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;

  f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) ;

  g) la protection de la personne concernée ou des droits et libertés d'autrui.

32 En outre, l'objectif poursuivi par les mesures relevant de l'article 15 « **doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux** » (point 115).

13. Voir la section 2 page 10 du mémoire ampliatif du 27 novembre 2015.

33 Ainsi, *en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales*, la **lutte contre la criminalité grave** est **le seul objectif d'intérêt général** susceptible de justifier une mesure de conservation de données de connexion, dès lors qu'une telle mesure constitue une ingérence particulièrement grave (point 102 de l'arrêt *Tele2*). [14]

34 Par analogie, en matière de protection des droits et libertés d'autrui, seule la protection des droits et libertés les plus importants et pour lesquels les dommages sont les plus graves et irréversibles est susceptible de justifier une mesure de conservation de données de connexion, dès lors que l'objectif poursuivi doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cette conservation.

35 **En l'espèce,** les mesures françaises imposant la conservation de données de connexion ne sont nullement limitées à la poursuite d'un objectif de lutte contre la criminalité grave en matière pénale. [15]

36 D'une part, l'article L. 34-1, III, CPCE dispose que

> « Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. [...] »

37 D'autre part, l'article 6, II, LCEN dispose que :

> « Les personnes mentionnées aux 1 et 2 du I 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. [...]
>
> « L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa. »

38 Il ressort de ces dispositions que :

- elles concernent :
  - toutes infractions pénales (**sans limitation aux seules infractions relevant de la criminalité grave**), mais aussi

14. Voir également la section 3 page 5 du mémoire en réplique du 22 juillet 2016.
15. Voir la section 2 page 10 du mémoire ampliatif du 27 novembre 2015.

— tous manquements à une obligation de surveillance de son accès à Internet dépourvue de caractère pénal (article L. 336-3, alinéa 2, du code de la propriété intellectuelle) ;
— elles ont pour but de permettre (**y compris pour des objectifs indéterminés**) toute réquisition de l'autorité judiciaire, y compris des tribunaux civils, mais également de nombreuses autorités administratives, y compris l'ANSSI et la Hadopi (qui sont explicitement visées par les dispositions litigieuses) ainsi que d'autres autorités, notamment : l'AMF (L. 621-10 du code monétaire et financier), les autorités fiscales (L96 G du livre des procédures fiscales), les douanes (art. 65 du code des douanes), les services de renseignement, etc. notamment pour des objectifs relevant de la prévention de la criminalité, sans limitation au domaine de la lutte contre la criminalité grave.

39 Ainsi, force est de constater que, tant l'article L. 34-1, III, CPCE que l'article 6, II, LCEN poursuivent de nombreux et larges objectifs, mais que :

— certains de ces objectifs ne sont pas compris dans la liste exhaustive des objectifs d'intérêt général susceptibles de justifier une mesure relevant du champ d'application de l'article 15 de la directive 2002/58, et que
— aucun de ces objectifs n'est en relation avec la gravité de l'ingérence dans les droits fondamentaux que constitue la conservation des données de trafic et de localisation et d'autres données afférentes aux communications.

40 **En conséquence,** les objectifs poursuivis par les dispositions litigieuses en matière pénale ne sont pas limités à la lutte contre la criminalité grave. Les autres objectifs poursuivis (i) soit ne sont pas susceptibles de justifier une conservation des données relatives aux communications, (ii) soit ne sont pas suffisamment limités. Partant, ces objectifs ne sauraient en aucun cas justifier une ingérence aussi grande dans les droits fondamentaux que celle causée en l'espèce.

41 Pour cette raison, déjà, le Conseil d'État doit faire droit à la demande d'abrogation des dispositions règlementaires, en ce qu'elles méconnaissent les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne.

42 En outre, un régime de conservation préventive des données de connexion, même justifié par la lutte contre la criminalité grave, ne saurait être considéré comme compatible avec la Charte sans respecter les exigences de stricte nécessité explicitées dans ce contexte et sans ambiguïté par la Cour de justice dans l'arrêt *Tele2*.

4. Sur l'absence de stricte nécessité des régimes français de conservation généralisée des données

43 **En second lieu**, les dispositions de l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et du décret n° 2011-219 du 25 février 2011 pris en application de la loi n° 2004-575 du 21 juin 2004 (LCEN) méconnaissent les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne en ce qu'elles organisent les régimes français de conservation des données de connexion en s'abstenant de les limiter au strict nécessaire.

44 Ce faisant, ces dispositions et celles sur lesquelles elles se fondent entraînent de nombreux et substantiels manquements aux exigences de respect de la Charte dès lors qu'elles s'appliquent systématiquement, en toutes circonstances et en tous lieux ; qu'elles concernent tous les moyens de communications électroniques et de communication au public en ligne ; qu'elles couvrent la quasi-totalité de la population, et qu'elles ne sont limitées par aucun critère objectif en rapport avec la finalité poursuivie.

45 **En droit,** un régime de conservation des données de connexion qui ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi excède les limites du strict nécessaire et ne saurait être considéré comme justifié dans une société démocratique ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58 lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragaphe 1, de la Charte (cf. points 105 à 107 de l'arrêt *Tele2* ; points 57 à 59 de l'arrêt *Digital Rights* ; mais aussi CJUE, g^de^ ch., 6 oct. 2015, *Schrems*, C-362/14, point 93). [16]

46 En particulier, aux fins de lutte contre la criminalité grave, excède forcément les limites du strict nécessaire un régime de conservation des données qui :

- « ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique » (point 106 de l'arrêt *Tele2* et point 59 de l'arrêt *Digital Rights*) ;
- « n'est pas limité à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité » (*ibid*) ;
- « concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales » (point 105 de l'arrêt *Tele2* et point 58 de l'arrêt *Digital Rights*) ;

16. Voir la section 4 page 15 du mémoire ampliatif du 27 novembre 2015, ainsi que la section 4 page 6 du mémoire en réplique du 22 juillet 2016.

— s'applique « même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves » (*ibid*) ; ou
— « ne prévoit aucune exception pour les communications des personnes soumises au secret professionnel » (*ibid*).

47 Pour autant, le droit européen ne s'oppose pas à ce qu'une réglementation permette, à titre préventif, la conservation **« ciblée »** des données de connexion, « à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées *ainsi que* la durée de conservation retenue, limitée au strict nécessaire » (point 108 de l'arrêt *Tele2*).

48 Pour que *chacune* de ces exigences de limitation au strict nécessaire soient garanties, la Cour de justice considère qu'il faut :

> « [...] en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle ***doit*** en particulier **indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise**, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 54 et jurisprudence citée).
>
> « En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en ***doit*** pas moins **toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi**. En particulier, de telles conditions ***doivent*** **s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné**.
>
> « S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale ***doit*** **être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque**

> **grave pour la sécurité publique**. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes. »
>
> (points 109 à 111 de l'arrêt *Tele2*)

49 **En l'espèce,** les régimes français imposant la conservation des données de connexion ne prévoient aucune limitation, différenciation ni exception à même de garantir leur limitation au strict nécessaire à la poursuite d'un objectif d'intérêt général.

50 Au contraire, les règles et limitations des régimes français sont largement insuffisantes et incompatibles avec les exigences de stricte nécessité que le respect de la Charte demande.

51 En particulier, tout d'abord, les régimes français de conservation des données de connexion ne prévoient aucune exception pour les personnes soumises au secret professionnel.

52 Ensuite, les régimes français de conservation des données de connexion sont applicables systématiquement, en toutes circonstances et en tous lieux. Ils ne sont donc pas limités à des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité. Ce constat vaut également pour d'autres objectifs.

53 Les listes des données de connexion à conserver (faites par les dispositions règlementaires dont l'abrogation est demandée) sont établies sans qu'aucun critère objectif ne permette de déterminer leur rapport avec l'objectif poursuivi. Ces dispositions ne requièrent donc pas qu'il existe une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. En pratique, ces listes de données à conserver ne délimitent aucunement l'ampleur de la mesure de conservation, de telle sorte qu'elles concernent tous les abonnés et utilisateurs, pour la totalité des services de communications électroniques ou de communication au public en ligne soumis au droit français, pour une durée d'un an, et ce, quel que soit l'objectif éventuellement poursuivi.

54 Enfin, les régimes français de conservation des données de connexion couvrent de manière généralisée l'ensemble des abonnés et utilisateurs de services de communications électroniques, ainsi que l'ensemble des utilisateurs de services de communication au public en ligne, sans que ces personnes se trouvent — ne serait-ce qu'indirectement — dans une situation susceptible de donner lieu à des poursuites pénales. Les régimes français s'appliquent donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. Elles ne contribuent pas non plus d'une manière ou d'une autre à la lutte contre la criminalité grave, ou de

prévenir un risque grave pour la sécurité publique. Au contraire, ces régimes imposent la conservation des données de connexion de la quasi-totalité de la population française.

55 Et pour cause, la volonté du législateur français — défendue par le Gouvernement à l'audience devant la grande chambre de la Cour de justice [17, 18] — consiste à conserver préventivement des données sur la quasi-totalité de la population puisqu'il est impossible de déterminer, *a priori*, quelles personnes seraient susceptibles, à l'avenir, de présenter un intérêt ou être en lien avec une infraction grave.

56 En somme, les régimes français de conservation de données de connexion relèvent d'une logique de suspicion généralisée intrinsèquement incompatible avec les droits au respect de la vie privée et à la protection des données personnelles et avec la protection de la liberté d'expression.

57 **En conséquence,** les régimes français de conservation des données de connexion ne sont pas limités au strict nécessaire en raison des nombreux manquements aux exigences de respect de la Charte : ils s'appliquent systématiquement, en toutes circonstances et en tous lieux ; ils concernent tous les moyens de communications électroniques et de communication au public en ligne ; ils couvrent la quasi-totalité de la population, et ils ne sont limités par aucun critère objectif en rapport avec l'objectif poursuivi — chacun de ces motifs démontrant l'absence de garantie de limitation au strict nécessaire.

58 Pour ces raisons, le Conseil d'État doit faire droit à la demande d'abrogation des dispositions règlementaires litigieuses, (i) en raison des manquements de ces dispositions aux exigences de respect de la Charte, et (ii) en ce qu'elles sont dépourvues de base légale en raison de l'incompatibilité des dispositions législatives dont elles découlent avec le respect des droits fondamentaux garantis par la Charte.

17. Marc Rees, « L'obligation de conservation des données de connexion auscultée par la CJUE », https://www.nextinpact.com/news/99520-l-obligation-conservation-donnees-connexion-auscultee-par-cjue.htm, 18 avril 2016

18. Vesela Gladicheva, « Tele2 challenges data-retention law at EU court, citing risk of 'misuse' », MLex, 13 avril 2016 ; voir notamment :

> *Lawyers for [...] France echoed those views during the hearing. Data retention must be general if it's meant to help fight crime. [...] Denmark's lawyer said it was "impossible to know beforehand which data might prove relevant," a view backed by France [...].*
>
> [Traduction par nos soins :]
>
> Les juristes représentant la France ont fait écho à ces points de vue lors de l'audience. La conservation des données doit être générale afin de contribuer à la lutte contre la criminalité. [...] Le juriste du Danemark a dit qu'« il est impossible de savoir a priori quelles données seront pertinentes », un point de vue soutenu par la France [...].

Par ces motifs, et tous autres à produire, déduire, suppléer, au besoin même d'office, les association requérantes persistent et concluent à ce que le Conseil d'État :

— ANNULE la décision attaquée ;
— ENJOIGNE à l'administration d'abroger l'article R. 10-13 du code des postes et communications électroniques et le décret n° 2011-219 du 25 février 2011 ;
— CONSTATE la contrariété des articles L. 34-1, III, CPCE ainsi que 6, II, LCEN avec l'article 15, paragraphe 1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne ;
— METTE À LA CHARGE de l'État le versement de la somme de 1024 € sur le fondement de l'article L. 761-1 du code de justice administrative.

Le 1er février 2017 à Paris,

Pour les associations requérantes, le mandataire unique

Benjamin BAYART

TABLE DES JURISPRUDENCES

ANNEXE : TABLEAU COMPARATIF (DROIT SUÉDOIS / DROIT FRANÇAIS)

	Le droit suédois ***(points 17 et 18 de l'arrêt* Tele2*)***	**Le droit français** **L. 34-1 & R. 10-13 CPCE & art. 6, II LCEN & D. 2011-219**
Intermédiaires concernés par l'obligation de conservation	fournisseurs de services de communications électroniques	toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ; (L. 34-1) toute personne physique ou morale fournissant au public un service de communications électroniques ; (L. 34-1) les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ; (L. 34-1 & LCEN) toute personne qui, au titre d'une activité professionnelle principale ou accessoire, offre au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit ; (L. 34-1) les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services. (LCEN)

	Le droit suédois ***(points 17 et 18 de l'arrêt* Tele2*)***	**Le droit français** **L. 34-1 & R. 10-13 CPCE & art. 6, II LCEN & D. 2011-219**
Définition générale des données conservées	données générées ou traitées dans le cadre d'un service de téléphonie, d'un service de téléphonie par un point de connexion mobile, d'un système de messagerie électronique, d'un service d'accès à Internet ainsi que d'un service de fourniture de capacités d'accès à Internet (mode de connexion)	données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation (L. 34-1 et L. 32, 18° CPCE) ; informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi (R. 10-12 CPCE) ; 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 (service d'accès à des services de communication au public en ligne ou services pour mise à disposition du public par des services de communication au public en ligne) (LCEN, art. 6).

	Le droit suédois ***(points 17 et 18 de l'arrêt* Tele2*)***	**Le droit français** **L. 34-1 & R. 10-13 CPCE & art. 6, II LCEN & D. 2011-219**
Détails des données conservées :	données relatives aux **abonnements**	données relatives aux **services complémentaires** demandés ou utilisés et leurs fournisseurs (R. 10-13) identifiant de connexion au moment de la **création du compte** ; (D.2011-219) nom et prénom ou la raison sociale ; (D.2011-219) adresses postales associées ; (D.2011-219) pseudonymes utilisés ; (D.2011-219) adresses de courrier électronique ou de compte associées ; (D.2011-219) numéros de téléphone ; (D.2011-219) données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour ; (D.2011-219) type de paiement utilisé ; (D.2011-219) référence du paiement ; (D.2011-219) montant ; (D.2011-219) date et l'heure de la transaction (D.2011-219).

	Le droit suédois ***(points 17 et 18 de l'arrêt* Tele2*)***	**Le droit français** **L. 34-1 & R. 10-13 CPCE & art. 6, II LCEN & D. 2011-219**
	données relatives à toutes communications nécessaires pour retrouver et identifier la **source** et la **destination** d'une communication (téléphonie uniquement) données relatives aux appels et aux numéros appelés (téléphonie sur IP) **adresses IP** de l'appelant et de l'appelé (accès Internet) données relatives aux **adresses IP** des utilisateurs	caractéristiques techniques des communications (L. 34-1, VI) informations permettant d'identifier **l'utilisateur** ; (R. 10-13) données permettant d'identifier le ou les **destinataires** de la communication (R. 10-13) **identifiant de la connexion** [à l'origine de la communication] (D.2011-219) **identifiant** attribué à **l'abonné** / au contenu (D.2011-219) identifiant utilisé par l'auteur de l'opération (D. 2011-219)
	données relatives à toutes communications nécessaires pour déterminer la **date, l'heure, la durée** et **la nature** d'une communication (téléphonie uniquement) dates et heures traçables de **début** et **d'achèvement** de la communication ; dates et heures traçables de **connexion** et de **déconnexion** au service d'accès à Internet ;	caractéristiques techniques ainsi que la **date**, **l'horaire** et la **durée** de chaque communication (L. 34-1, VI & R. 10-13) dates et heure de début et de fin de la **connexion** / date et heure de **l'opération** (D.2011-219) **nature** de l'opération (D.2011-219)
	données relatives à toutes communications nécessaires pour identifier le **matériel** de communication	caractéristiques techniques des communications (L. 34-1, VI) données relatives aux **équipements terminaux** de communication utilisés ; (R. 10-13) identifiant du **terminal** utilisé pour la connexion (D.2011-219) caractéristiques de la **ligne** de l'abonné (D.2011-219)

	Le droit suédois ***(points 17 et 18 de l'arrêt* Tele2*)***	**Le droit français** **L. 34-1 & R. 10-13 CPCE & art. 6, II LCEN & D. 2011-219**
	données relatives à toutes communications nécessaires pour **localiser** le matériel de communication mobile utilisé au début et à l'achèvement de la communication	données portant sur la **localisation** des équipements terminaux (L. 34-1, VI) (activités de téléphonique uniquement) données permettant d'identifier **l'origine** et la **localisation** de la communication (R. 10-13, II)
Exclusion des données conservées	L'obligation de conservation des données **ne porte** cependant **pas sur le contenu des communications**	données ne pouvant **en aucun cas porter sur le contenu** des correspondances échangées ou des **informations consultées**, sous quelque forme que ce soit, dans le cadre de ces communications (L. 34-1, VI) données qui **ne peuvent porter sur le contenu** de correspondances ou les **informations consultées** (Conseil constitutionnel, Décision n° 2015-478 QPC du 24 juillet 2015, Association French Data Network et autres [Accès administratif aux données de connexion])
Durée de conservation	pendant **six mois** à compter du jour de l'achèvement de la communication	pour une durée maximale d'**un an** (L. 34-1, III) à compter du jour de l'enregistrement (R. 10-13, III) La durée de conservation des données [. . .] est d'**un an**, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu ; à compter du jour de la résiliation du contrat ou de la fermeture du compte ; à compter de la date d'émission de la facture ou de l'opération de paiement (selon les cas ; cf. art. 3, D2011-219)