# Faits et procédure

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 no 2011-219 du 25 février 2011 pris en application de la loi no 2004-575 du 21 juin 2004 (LCEN) comme étant contraires à la Charte des droits fondamentaux de l’Union européenne (la Charte) et à la directive 2002/58/CE de l’Union européenne. Le 6 juillet 2015, le Gouvernement a tacitement refusé d’abroger ces dispositions, alors même qu’un double changement de circonstances l’exigeait.[[1]](#footnote-2)

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](https://exegetes.eu.org/recours/abrogationretention/CEtat/2016-02-08-Tierce-Intervention-FR.pdf).

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](https://exegetes.eu.org/recours/abrogationretention/CEtat/2016-07-22-replique.pdf).

Les associations requérantes persistent dans l’ensemble des moyens et des conclusions qu’elles ont développés dans leurs précédentes écritures. Elles entendent désormais, par la production du présent mémoire, mettre en évidence la motivation de l’arrêt de la grande chambre de la Cour de justice du 21 décembre 2016[[2]](#footnote-3), laquelle confirme amplement le bien-fondé de la demande d’abrogation des dispositions litigieuses adressée au gouvernement.

# Discussion

Après avoir rappelé que les dispositions litigieuses relèvent du champ d’application du droit de l’Union européenne lu à la lumière de la Charte des droits fondamentaux (section #directive200258), les associations requérantes démontrent en quoi leur demande d’abrogation est fondée en raison, d’abord, de l’ingérence particulièrement grave que cause le droit français en matière de conservation des données de connexion (section #ingerence); une ingérence d’une telle gravité ne pouvant pas être justifiée par des objectifs aussi larges ou indéfinis que ceux du droit français, lesquels ne sont nullement limités à la lutte contre la criminalité grave (section #objectif).

Enfin, les associations requérantes insistent sur la motivation sans ambiguité de la grande chambre de la Cour de justice, qui pose les exigences de respect du strict nécessaire pour toutes mesures de conservation des données de connexion relevant de la directive 2002/58 — exigences qu’un régime de conservation généralisée tel que ceux prévus en droit français ne respecte pas (section #strict).

## Sur le champ d’application de la directive 2002/58

**En droit,** relève du champ d’application de la directive 2002/58, toute mesure législative qui impose la conservation de données de connexion ou permettant l’accès à de telles données, dès lors que ces activités impliquent nécessairement le traitement de données à caractère personnel (CJUE, gde ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, points 73, 75 et 76 notamment).

Sont concernées en particulier des mesures législatives imposant la conservation des données à des fournisseurs de services de communications électroniques, mais également toutes mesures imposant la conservation de données de connexion par toute autre entité, puisque 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)

**En l’espèce,** il n’est pas contesté que les données de connexion conservées par les opérateurs et personnes mentionnées aux articles L. 34-1 CPCE et 6, I, 1 et 2, LCEN doivent être considérées comme des données à caractère personnel. Dès lors, les dispositions litigieuses imposant la conservation de données de connexion impliquent nécessairement le traitement de données à caractère personnel et ce, que la personne concernée ait pu donner son consentement ou non.

Pour rappel, les « données de connexion » en droit français se rapportent non seulement aux « données relatives au trafic » mais aussi aux « données de nature à permettre l’identification de quiconque a contribué » à un contenu en ligne. Mais en réalité, la liste des données faite au décret no 2011-219 contient des données relatives au trafic (par exemple, l’identifiant de la connexion à l’origine de la communication). [¶connexion]

Par ailleurs, on peut relever que l’article 6, II, LCEN impose non seulement la conservation, mais également la détention de données de connexion, de telle sorte que cette disposition impose aux fournisseurs d’accès de détenir des données afférentes à ces communications sans que de telles données soient techniquement nécessaires à l’acheminement de ces communications.

En conclusion, il ne peut être contesté que les dispositions litigieuses impliquent la détention et la conservation de données afférentes à des communications électroniques, à l’insu de l’utilisateur de services de communication au public en ligne abonné à un service de communication électronique. Ainsi, ces dispositions entravent la confidentialité des communications électroniques.

**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.

Partant, les dispositions litigieuses doivent être compatibles avec cette directive, lue à la lumière de la Charte, notamment ses articles 7, 8, 11 et 52.[[3]](#footnote-4)

## Sur la particulière gravité et l’ampleur de l’atteinte aux droits fondamentaux causée par les dispositions litigieuses

**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),[[4]](#footnote-5) 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 et 101 de l’arrêt précité)[[5]](#footnote-6).

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 aux points 256 et s. de ses conclusions dans l’affaire *Tele2*, « à la différence de mesures de surveillance ciblées, une telle obligation est **susceptible de faciliter considérablement les ingérences de masse**, c’est-à-dire les ingérences affectant une partie substantielle ou même l’ensemble de la population pertinente. » Il ajoute notamment 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 » (CJUE, 19 juill. 2016, *Conclusions de l’avocat général M. Henrik Saugmandsgaard Øe*, C-203/15, C-698/15).

La Cour conclut à nouveau (cf. CJUE, gde 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 :

« 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. l’avocat général aux points 253, 254 et 257 à 259 de ses conclusions, 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*)

Par ailleurs, un tel sentiment de surveillance constante implique nécessairement une atteinte à la liberté d’expression; suivant la jurisprudence de la Cour EDH, une telle mesure :

« crée par sa simple existence, pour tous ceux auxquels on pourrait l’appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications. »

(Cour EDH, Plén., 6 sept. 1978, *Klass c. All.*, no 5029/71, §41 : voir aussi Cour EDH, 26 mars 1987, *Leander c. Suède*, no 9248/81, §48 : Cour EDH, 4 mai 2000, *Rotaru c. Roumanie*, no 28341/95, §46)

**En l’espèce,** l’ingérence constituée par les dispositions françaises est encore plus grande et plus vaste que celle constituée par la directive 2006/24[[6]](#footnote-7) ou que celle constituée par le droit suédois ou anglais, en raison du champ plus large des données conservées et du champ plus large des personnes soumises à l’obligation de conservation (cf. connexion).

**En conséquence,** il ne saurait être contesté que la conservation des données de connexion prévue en droit française 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 communication électronique.

## Sur l’objectif d’intérêt général susceptible de justifier la conservation des données

**En droit,** seule la lutte contre la criminalité grave est susceptible de justifier une mesure de conservation de données de connexion, dès lors qu’une telle mesure constitue une ingérence particulièrement grave et de grande ampleur (point 102 de l’arrêt *Tele2* et point 60 de l’arrêt *Digital Rights* précité)[[7]](#footnote-8).

**En l’espèce,** les mesures françaises imposant la conservation de données de connexion ne sont nullement limitées à la poursuite d’un objectif limité à la lutte contre la criminalité grave.[[8]](#footnote-9)

En premier lieu, l’article L. 34-1 CPCE dispose en son point III 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. […] »

En second lieu, l’article 6 LCEN dispose en son point II 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. »

Il ressort de ces dispositions que la conservation des données de connexion n’est en aucun cas réservée à la lutte contre la criminalité grave puisque :

* elles concernent : toutes infractions pénales (sans limitation aux seules infractions relevant de la criminalité grave) ainsi que tous manquemants à une obligation dépourvue de caractère pénal (article L. 336-3, alinéa 2, du code de la propriété intellectuelle);
* elles ont pour but de permettre toute réquisition de l’autorité judiciaire, y compris des tribunaux civils, mais également de nombreuses autorités administratives — 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. — sans limitation au domaine de la lutte contre la criminalité grave.

**En conséquence,** l’objectif poursuivi par les dispositions litigieuses n’est pas limité à la lutte contre la criminalité grave. Partant, l’objectif poursuivi les dispositions litigieuses ne saurait en aucun cas justifier une ingérence aussi grande dans les droits fondamentaux que celle causée en l’espèce.

Pour cette raison, déjà, le Conseil d’État doit faire droit à la demande d’abrogation des dispositions règlementaires litigieuses, en ce qu’elles sont dépourvues de base légale en raison de leur poursuite d’un objectif au-delà d’un objectif d’intérêt général permettant de justifier l’ingérence en cause dan les droits fondamentaux garantis par la Charte.

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 sans ambiguité par la Cour de justice dans l’arrêt *Tele2*.

## Sur l’absence de stricte nécessité des régimes français de conservation généralisée des données

**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 considérée 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, parargaphe 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, gde ch., 6 oct. 2015, *Schrems*, C-362/14, point 93).[[9]](#footnote-10)

En particulier, 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*);
* « s’applique 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 » (*ibid*); ou
* « ne prévoit aucune exception pour les communications des personnes soumises au secret professionnel » (*ibid*).

Pour autant, aux fins de lutte contre la criminalité grave, le droit européen ne s’oppose pas à une réglementation permettant, 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*)

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*)

**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. 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.

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.

Ensuite, les régimes français de conservation des données de connexion sont applicables systématiquement, en toutes circonstances et en tous lieux; de telle sorte qu’ils ne sont 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.

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; de telle sorte qu’ils ne requièrent aucune 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 communication électronique 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.

Enfin, les régimes français de conservation des données de connexion couvrent de manière généralisée l’ensemble des abonnés et utilisateurs de services de communication électronique, ainsi que l’ensemble des utilisateurs de services de communication au public en ligne, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales; de telle sorte qu’ils s’appliquent 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, 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 — au contraire, ils concernent la quasi-totalité de la population française.

Et pour cause, la volonté du législateur — défendue par le gouvernement à l’audience devant la grande chambre de la Cour de justice[[10]](#footnote-11),[[11]](#footnote-12) — consiste à conserver préventivement des données sur la quasi-totalité de la population puisqu’il est impossible, *a priori*, de déterminer quelles personnes seraient susceptibles, à l’avenir, de présenter un intérêt ou être un lien avec un objectif poursuivi par les autorités.

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

**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 communication électronique 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.

Pour ces raisons, le Conseil d’État doit faire droit à la demande d’abrogation des dispositions règlementaires litigieuses, 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.

\* \* \*

**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 le décret no 2011-219 du 25 février 2011 et l’article R. 10-13 du code des postes et communications électroniques :
* 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.

Avec toutes conséquences de droit.

\* \* \*

Le FIXME à Paris,

Pour les associations requérantes, le mandataire unique

Benjamin Bayart

\* \* \*\* \* \*

# Table des jurisprudences

CJUE, gde ch., 8 avr. 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres*, C-293/12, C-594/12

CJUE, gde ch., 6 oct. 2015, *Maximilian Schrems contre Data Protection Commissioner*, C-362/14

CJUE, gde ch., 21 déc. 2016, *Tele2 Sverige AB c. Postoch telestyrelsen et Secretary of State for the Home Department*, C-203/15, C-698/15

Cour EDH, Plén., 6 sept. 1978, *Klass et autres c. Allemagne*, no 5029/71

Cour EDH, 26 mars 1987, *Leander c. Suède*, no 9248/81

Cour EDH, 4 mai 2000, *Rotaru c. Roumanie*, no 28341/95

1. voir la section 2 page 4 du [mémoire ampliatif du 27 novembre 2015](https://exegetes.eu.org/recours/abrogationretention/CEtat/2015-11-27-complement1.pdf) [↑](#footnote-ref-2)
2. CJUE, gde ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15 [↑](#footnote-ref-3)
3. voir à ce sujet le [mémoire complémentaire sur l’applicabilité de la Charte des droits fondamentaux de l’Union européenne produit par les associations requérantes le 17 mai 2016](https://exegetes.eu.org/recours/abrogationretention/CEtat/2016-05-17-complement-charte.pdf) [↑](#footnote-ref-4)
4. voir la section 1 page 7 du [mémoire ampliatif du 27 novembre 2015](https://exegetes.eu.org/recours/abrogationretention/CEtat/2015-11-27-complement1.pdf) [↑](#footnote-ref-5)
5. voir également la section 2 page 4 du [mémoire en réplique du 22 juillet 2016](https://exegetes.eu.org/recours/abrogationretention/CEtat/2016-07-22-replique.pdf) [↑](#footnote-ref-6)
6. voir, notamment, la section 1.2 page 9 du [mémoire ampliatif du 27 novembre 2015](https://exegetes.eu.org/recours/abrogationretention/CEtat/2015-11-27-complement1.pdf) [↑](#footnote-ref-7)
7. voir également la section 3 page 5 du mémoire en réplique du 22 juillet 2016 [↑](#footnote-ref-8)
8. voir la section 2 page 10 du [mémoire ampliatif du 27 novembre 2015](https://exegetes.eu.org/recours/abrogationretention/CEtat/2015-11-27-complement1.pdf) [↑](#footnote-ref-9)
9. voir la section 4 page 15 du [mémoire ampliatif du 27 novembre 2015](https://exegetes.eu.org/recours/abrogationretention/CEtat/2015-11-27-complement1.pdf), ainsi que la section 4 page 6 du [mémoire en réplique du 22 juillet 2016](https://exegetes.eu.org/recours/abrogationretention/CEtat/2016-07-22-replique.pdf) [↑](#footnote-ref-10)
10. 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 [↑](#footnote-ref-11)
11. 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 pour la France ont fait écho de ce point de vue à l’audience. La conservation des données doit être générale aux fins de contribuer à la lutte contre la criminalité. […] Le juriste du Danmark a dit qu’« il est impossible de savoir a priori quelles données seront pertinentes », un point de vue suivi par la France […]. [↑](#footnote-ref-12)