**SPINOSI & SUREAU**
SCP d'Avocat au Conseil d'Etat
et à la Cour de cassation
16 Boulevard Raspail
75007 PARIS

# CONSEIL D'ÉTAT

## SECTION DU CONTENTIEUX

## OBSERVATIONS COMPLEMENTAIRES

POUR **:** **1/ La Quadrature du Net**

**2/ French Data Network**

**3/ La Fédération des fournisseurs d'accès à Internet associatifs**

*SCP SPINOSI & SUREAU*

CONTRE **:** 1/ Le Premier ministre

2/ Ministre de l'intérieur

3/ Ministre des armées

**Sur la requête n° 397.851**

**I.** Persistant dans l'ensemble des moyens et conclusions développés dans ses précédentes écritures, les associations exposantes entendent présenter les observations complémentaires suivantes, notamment aux fins de répliquer aux observations ministérielles et soulever les moyens complémentaires suivants.

**II. A titre liminaire**, les associations rappellent qu'à la suite de la question prioritaire de constitutionnalité qu'elles ont posé à l'encontre des dispositions de l'article L. 811-51 du code de la sécurité intérieure, le Conseil constitutionnel a censuré ces dispositions aux motifs qu'elles portent « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (Conseil constit., Déc. n° 2016-590 QPC du 21 octobre 2016).

**Sur l'applicabilité de la Charte des droits fondamentaux de l'Union européenne**

**III. En premier lieu**, les associations exposantes tiennent à réaffirmer pleinement que les mesures attaquées entrent résolument dans le champ d'application du droit de l'Union, de sorte que la Charte des droits fondamentaux de l'Union européenne ainsi que les autres instruments de droit dérivés – en particulier la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur – sont bien invocables dans le présent litige.

**III-1** En effet, force est de constater que ces assertions ont été directement et indiscutablement confirmées par la Cour de justice de l'Union européenne, dans l'arrêt *Tele 2*, tant sur le champ d'application du droit de l'UE et de la Charte, que sur l'interprétation de l'article 15 de la directive 2002/58 (CJUE, g$^{de}$ ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15).

Ainsi, la Cour de justice a très clairement énoncé que :

« *Eu égard à l'économie générale de la directive 2002/58, les éléments relevés au point précédent du présent arrêt n'autorisent pas à conclure que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 seraient exclues du champ d'application de cette directive, sauf à priver cette disposition de tout effet utile.*

*En effet, ladite disposition présuppose nécessairement que les mesures nationales qui y sont visées, telles que celles relatives à la conservation de données à des fins de lutte contre la criminalité, relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit* » (CJUE, g$^{de}$ ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, point 73).

Ainsi, les mesures entravant l'article 5 de la directive 2002/58 pour les motifs énoncés à l'article 15, paragraphe 1, de la même directive tombent nécessairement dans le champ d'application du droit de l'Union.

Plus précisément, la grande chambre de la Cour de justice a décidé que :

« *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*** (§ 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 […]* » (§ 85).

L'article 5 de la directive 2002/58 s'applique donc pleinement aux mesures des autorités nationales ayant pour objet l'accès aux données de connexion ainsi qu'aux mesures d'interception du contenu des réseaux de communications électroniques.

Dès lors, de telles mesures nationales relèvent du champ d'application du droit de l'Union et doivent, pour cette raison, être limitées au strict nécessaire conformément aux exigences de la Charte, lesquelles sont parfaitement opposables à ces mesures nationales.

**III-2** Or, en l'occurrence, la plupart des techniques de recueil de renseignement instituées par la loi du 24 juillet 2015 et ses décrets d'application portent sur des accès aux communications électroniques transmises sur des réseaux de communications électroniques.

Cela vaut notamment pour toutes les mesures de surveillance internationale, de recueil de données de connexion, d'accès aux données de connexion en temps réel, de traitements algorithmiques sur des données de connexion ou encore d'interceptions de sécurité.

Dès lors, il ne fait aucun doute que les mesures en cause ont pour objet principal — si ce n'est exclusif — l'accès aux données des communications électroniques, qu'il s'agisse du contenu ou de métadonnées, notamment celles traitées et acheminées sur des réseaux de communications électroniques visés par la mise en œuvre de techniques de renseignement.

L'entrave que ces mesures constituent au regard du principe de confidentialité desdites communications est affirmée de manière constante et sans aucune ambiguïté par la Cour de justice.

**III-3 Par conséquent,** les techniques de recueil de renseignements en cause doivent être conformes au droit de l'Union et notamment aux directives 2000/31 et 2002/58 interprétées à la lumière de la Charte ainsi qu'aux articles 7, 8, 11 et 52, paragraphe 1, de la Charte elle-même.

À ce titre, les associations exposantes ne peuvent que renvoyer à leurs observations relatives à la disproportion des dispositions attaquées (cf. **observations complémentaires aux points IX et s.**).

En tout état de cause, les exposantes rappellent que si le Conseil d'État venait à s'interroger sur les modalités d'application du droit de l'Union en l'espèce, celui-ci serait alors tenu de transmettre à la Cour de justice les questions correspondantes telles que formulées par les parties requérantes (cf. **le dispositif des observations complémentaires**).

**Sur la méconnaissance des exigences tirées des articles 8 et 13 de la Convention européenne des droits de l'homme concernant l'insuffisance des mécanismes compensant l'absence de notification *a posteriori***

**IV. En deuxième lieu**, l'association exposante réaffirme que l'absence de mécanisme de notification *a posteriori* emporte violation des articles 8 et 13 de la Convention européenne des droits de l'homme.

**IV-1** Tout d'abord, ainsi que les parties requérantes l'ont déjà amplement démontré dans leurs précédentes écritures, aucun mécanisme de droit interne ne permet de compenser, comme requis par la Cour européenne des droits de l'homme, l'inexistence de la procédure de notification (cf. **mémoire complémentaire aux points VI-1 et s**.).

Non seulement, les personnes concernées ne disposent strictement d'aucune information telle que requise par la Cour européenne des droits de l'homme.

Mais en outre, le mécanisme d'information prévu par les articles L. 833-4 et L. 841-1 du code de la sécurité intérieure ne saurait passer pour « *une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations sur les interceptions* » (Cour EDH, g$^{de}$ ch., 4 déc. 2015, *Zakharov c. Russie*, n$^{o}$ 47143/06, § 298) au sens des exigences tirées des articles 8 et 13 de la Convention.

**IV-2** Ensuite, il suffit de distinguer le cas des mesures portant sur des communications nationales de celles portant sur des communications internationales pour faire apparaître que la conventionalité du dispositif n'est aucunement assurée.

**IV-2.1** S'agissant des mesures portant sur les communications nationales, les associations requérantes ont déjà démontré que la procédure instituée par les articles L. 773-1 et s. du code de la justice administrative ne respecte en rien le principe du contradictoire notamment en ce que l'administration, partie à la procédure, est maître de ce qui entre dans le champ du secret de la défense nationale et donc des éléments pouvant être partagés ou non avec la partie requérante.

Étant rappelé que, contrairement à d'autres États membres, aucun mécanisme de représentation par des avocats habilités au secret défense n'a été créé.

Ainsi, l'introduction du secret défense dans les procédures contentieuses, bien loin de constituer une avancée, n'est en réalité qu'un profond recul du procès équitable et ne saurait en tout état de cause compenser l'inexistence d'une notification des personnes concernées par les techniques de renseignement portant sur les communications nationales.

**IV-2.2** De manière tout à fait déterminante, les personnes concernées ne disposent d'absolument aucun recours en matière de surveillance internationale, ni d'aucune notification sur les techniques de renseignement portant sur leurs communications internationales transitant par des réseaux de communications électroniques visés à l'article L. 854-2 du code de la sécurité intérieure.

**IV-2.2.1** D'une part, l'article L. 854-1 du code de la sécurité intérieure dispose que la surveillance internationale « *est exclusivement régie par le présent chapitre* ».

La possibilité pour les justiciables de se tourner vers la Commission nationale de contrôle des techniques de renseignement et le Conseil

d'État n'est donc pas garantie par la loi lorsque sont en cause des mesures de surveillance internationale.

Cela est confirmé par l'article L. 854-9 du code de la sécurité intérieure qui, dans le chapitre « surveillance internationale » du code de la sécurité intérieure, dispose que :

« *Sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance n'est irrégulièrement mise en œuvre à son égard, la commission s'assure que les mesures mises en œuvre au titre du présent chapitre respectent les conditions qu'il fixe* ».

Cet article, qui reproduit l'article L. 833-4 précité, implique en effet que les articles L. 833-4 et L. 841-1 ne sont pas applicables au chapitre encadrant la surveillance internationale.

**IV-2.2.2** D'autre part, l'article L. 773-1 du code de justice administrative (CJA) implique que le Conseil d'État ne peut être saisi que sur le fondement de l'article L. 841-1.

L'absence de recours devant le Conseil d'État est confirmée par la jurisprudence du Conseil constitutionnel, selon lequel « *la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure* » (Conseil constit., 26 nov. 2015, *Loi surveillance internationale*, 2015-722 DC, cons. 18).

**Par conséquent,** il apparaît donc que deux catégories de personnes doivent être distinguées :

- Ceux utilisant des « numéros d'abonnement ou des identifiants techniques rattachables au territoire national » au sens de l'article L. 854-1 du code de la sécurité intérieure, lesquels bénéficient d'un droit au recours édulcoré et insuffisant au regard des exigences de la Cour européenne des droits de l'homme ;

- Les autres, ne bénéficiant d'absolument aucun droit.

Pourtant, la Cour européenne des droits de l'homme ne fait pas de distinction selon la nature des numéros ou identifiants utilisés.

Il importe d'ailleurs de relever que la formulation empruntée à l'article L. 854-1 du code de la sécurité intérieure est pour le moins spécieuse. À l'heure où une immense partie des communications est entièrement numérique et transite entre de multiples prestataires (fournisseur de messagerie en ligne, opérateur grand public, transitaire, etc.), la notion d'« *identifiant technique rattachable au territoire national* » est pour le moins inconsistante.

La notion demeure indéfinie et la distinction entre les deux formes de communication, déjà injustifiée, est dénuée de toute pertinence en pratique dans de nombreux contextes, notamment celui des communications électroniques transitant par Internet.

**En définitive**, le Conseil d'Etat ne pourra manquer de faire droit aux prétentions des exposantes.

**Sur la méconnaissance du droit à un recours effectif et du droit à un procès équitable**

**V. En troisième lieu**, les associations exposantes entendent attirer l'attention du Conseil d'Etat sur un récent arrêt rendu par la Grande Chambre de la Cour européenne des droits de l'homme qui vient conforter un peu plus encore leur démonstration selon laquelle les dispositions du livre VIII du code de la sécurité intérieure intitulé « *Du renseignement* » ainsi que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, portent atteinte au droit à un recours effectif et au droit à un procès équitable, dont dérive tout particulièrement le principe du contradictoire.

**V-1** En effet, et en droit, il importe de relever que la Cour européenne des droits de l'homme opère une mise en balance entre les droits des justiciables et les raisons soulevées par les Etats susceptibles de justifier la non-divulgation de certaines preuves pertinentes, telles que la sécurité nationale, afin de déterminer si le droit à un procès équitable n'a pas été méconnu.

A cet égard, et selon une jurisprudence désormais établie, si le droit à la divulgation des preuves n'est pas absolu, « *toutes difficultés causées à la défense par une telle limitation doivent être suffisamment compensées par la procédure suivie devant les autorités judiciaires* » (CEDH, g$^{de}$ ch., *Fitt c. Royaume-Uni*, Req. n° 29777/96, § 45). La Cour examine ainsi que « *le processus décisionnel a satisfait dans toute la mesure du possible aux exigences du contradictoire et de l'égalité des armes et s'il était assorti de garanties aptes à protéger les intérêts de l'accusé* » (*Ibid.* §46).

Une illustration d'un tel examen a été récemment et solennellement donnée par la Cour dans son arrêt *Regner c. République Tchèque* (CEDH, g$^{de}$ ch., 19 sept. 2017, Req. n°35289/11). Lorsque certains documents font l'objet d'une classification, de nouveaux critères sont fixés afin de rechercher « *si les limitations aux principes du contradictoire et de l'égalité des armes, tels qu'applicables dans la procédure civile, ont été suffisamment compensées par d'autres garanties procédurales* » (*Ibid.* §151), et ce, au regard du contrôle que possède l'autorité judiciaire sur les pièces classifiées.

Pour la Cour, la « *capacité des juges à apprécier les faits de l'espèce de manière adéquate* » n'a pu être remise en cause « *au motif qu'ils n'ont pas eu un accès intégral aux documents pertinents* » (*Ibid*. §152), car ceux-ci disposaient de garanties suffisantes, exhaustivement développées dans l'arrêt.

Ainsi, « *les tribunaux ont accès à tous les documents classifiés, sans restriction, sur lesquels l'Office s'est basé pour justifier sa décision. Ils ont ensuite le pouvoir de se livrer à un examen approfondi des raisons invoquées par l'Office pour ne pas communiquer les pièces classifiées. Ils peuvent en effet apprécier la justification de la non-communication des pièces classifiées et ordonner la communication de celles dont ils estimeraient qu'elles ne méritent leur classification* » (*Ibid*. §152).
La non-divulgation des preuves est donc compensée par la capacité des autorités judiciaires à examiner les motifs d'une mesure de renseignement, et à disposer d'un large pouvoir sur les pièces classées liées à cette mesure.

**V-2** Or, en l'occurrence, il est manifeste que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ne répondent pas à de telles garanties.

Plus précisément encore, il n'existe aucune compensation à la limitation au principe du contradictoire provoquée par le secret défense.

En effet, l'article L. 773-2 du code de justice administrative dispose notamment que « *dans le cadre de l'instruction de la requête, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement* ». Il n'est ainsi aucunement précisé si les pièces ayant justifié la mise en œuvre de la mesure de renseignement font partie des pièces connues par la formation de jugement.

Ensuite, les dispositions législatives ne permettent aucunement au juge de procéder à un examen approfondi des raisons invoquées par les autorités pour mettre en place une mesure de renseignement. En vertu de l'article L. 773-6 du code de justice administrative, le juge possède uniquement la capacité de constater une absence d'illégalité « *sans confirmer ni infirmer la mise en œuvre d'une technique* ».

Dans le cas d'une mesure déclarée illégale, l'article L.773-7 du code de justice administrative permet seulement au juge « *d'annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés* » sans, à nouveau, la soumettre à un examen approfondi.

Par ailleurs, l'article L.773-7 du même code dispose en son deuxième alinéa que « *sans faire état d'aucun élément protégé par le secret de la défense nationale, elle informe la personne concernée ou la juridiction de renvoi qu'une illégalité a été commise.* »

Il n'existe donc strictement aucune possibilité pour le juge d'assortir à cette information, la communication d'une pièce justifiant la mesure déclarée illégale.

Enfin, le troisième alinéa de l'article L.773-7 dispose que « *Lorsque la formation de jugement estime que l'illégalité constatée est susceptible*

*de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale, afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République ».*

Or, les avis de la Commission du secret de la défense nationale ne sont pas impératifs.

Si le juge peut éventuellement demander à ce qu'une pièce soit déclassifiée – étant rappelé qu'il ne sera pas nécessairement fait droit à une telle demande –, il ne peut en aucun cas l'ordonner.

**Par conséquent**, les dispositions en cause ne sont pas conformes aux exigences posées par la Cour européenne des droits de l'homme permettant de garantir le droit à un procès équitable.

De ce chef aussi, l'annulation des dispositions du décret litigieux s'impose faute de base légale.

**Sur l'extension du périmètre des données de connexion recueillies**

**VI. En quatrième lieu**, en autorisant l'autorité administrative à procéder au recueil en temps réel ou par détection automatique de données techniques autres que les seuls « *informations ou documents* » prévus à l'article L. 851-1, les dispositions litigieuses du décret ont méconnu l'étendue de la compétence règlementaire fixée par les articles 34 et 37 de la Constitution mais aussi porté atteinte au droit au respect de la vie privée constitutionnellement et conventionnellement garanti.

**VI-1 En droit,** il convient de rappeler qu'aux termes de l'article 34 de la Constitution : « *La loi fixe les règles concernant […] les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ».

Le législateur est ainsi exclusivement compétent pour définir les données de connexion pouvant être collectées par l'autorité

administrative, une telle collecte constituant une ingérence dans le droit au respect de la vie privée consacré à l'article 2 de la Déclaration de 1789 mais aussi à l'article 8 de la Convention européenne des droits de l'homme.

**VI-2** En l'occurrence, il convient de rappeler que les données de connexion pouvant être collectées par l'autorité administrative dans le cadre des finalités et procédures relatives au renseignement sont définies à l'article L. 851-1 du code de la sécurité intérieure.

Celui-ci dispose en son premier paragraphe :

« *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 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.* »

Cette disposition a par ailleurs fait l'objet d'un contrôle de constitutionnalité par le Conseil constitutionnel (Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC, cons. 55).

Le pouvoir réglementaire peut être amené à apporter des précisions pour la mise en œuvre de la loi — à condition toutefois que cela se fasse dans les limites de sa propre compétence au regard de l'article 34 de la Constitution et en cohérence avec les dispositions législatives telles qu'interprétées par le Conseil constitutionnel.

Or, au cas présent, le pouvoir réglementaire a manifestement méconnu l'étendue de sa compétence en ce qu'il a outrepassé les limites imparties

par l'article 34 de la Constitution dès lors que la liste des catégories de données fixée par le décret contrevient au sens et à la portée de la définition fixée par la loi.

Et ce, à plusieurs égards.

*Sur l'élargissement du périmètre des données auxquelles les autorités administratives peuvent désormais accéder*

**VI-2.1 Premièrement**, l'article 2, 3°, du décret 2016-67 crée une nouvelle section « *données de connexion susceptibles d'être recueillies* ».

Ce faisant, cet article élargit le périmètre des données auxquelles les autorités administratives peuvent désormais accéder, ce que la CNIL avait notamment critiqué.

Consultée pour avis lors de l'élaboration du décret, elle relève dans sa délibération n° 2015-455 du 17 décembre 2015, que « *les dispositions réglementaires qui lui sont soumises prévoient un élargissement des données pouvant être recueillies à ce titre* ». Elle relève également que « *la succession des dispositions législatives précitées et la refonte du code de la sécurité intérieure entraînent des modifications répétées et complexes des dispositions réglementaires, qui affectent leur lisibilité* ».

Cet élargissement est d'autant plus dommageable qu'il porte atteinte aux principes de confidentialité des communications électroniques et de secret des correspondances tels que consacrés, notamment, par les articles L. 34-1 et L. 32-3 du code des postes et des communications électroniques (CPCE), ainsi que par l'article 2 de la Déclaration de 1789. En tout état de cause, cette extension porte une atteinte nouvelle au droit au respect de la vie privée.

*De facto*, l'élargissement du périmètre des données de connexion nécessiterait dans certains cas la mise en œuvre de techniques dites de *deep packet inspection* (DPI) (en français inspection des paquets en profondeur), qui consistent en l'analyse des communications (y compris contenus et métadonnées) transitant sur les réseaux (parmi eux, notamment, Internet). Ces techniques d'inspection consistent à accéder,

non seulement, à des bribes de communication (au sein d'un seul paquet), mais aussi à l'intégralité d'une conversation (via l'analyse de flux, composés d'un ensemble de paquets).

Si l'on devait comparer ce procédé à une forme de communication non-électronique, il s'agirait par exemple d'ouvrir toutes les enveloppes transitant par la Poste afin d'en inspecter le contenu.

L'usage du procédé de *deep packet inspection* avait été dénoncé à l'Assemblée nationale. En effet, à l'occasion des débats parlementaires concernant le projet de loi relatif au renseignement, le ministre Bernard Cazeneuve, s'était fermement opposé à ce que la technique du *deep packet inspection* soit mise en œuvre :

*« [Il est] hors de question d'utiliser cette technique, et je le confirme. […] Nous n'utiliserons pas cette technique. C'est très clair. Je l'ai déjà dit au mois de novembre et je le répète aujourd'hui. Nous avons un processus très encadré qui consiste à prendre les données de connexion d'un groupe ciblé, d'où l'utilisation de la détection sur données anonymes. Si nous voulons entrer dans les communications, la procédure nous oblige à redemander l'autorisation à la CNCTR, et cette demande doit être fortement motivée. Nous n'utiliserons donc en aucun cas cette technique du DPI.* » (Compte rendu de la seconde séance de l'Assemblée Nationale, le mercredi 15 avril 2015. Compte rendu disponible en ligne : http://www.assemblee-nationale.fr/14/cri/2014-2015/20150217.asp - P517091 - Consulté au 23 novembre 2017).

Il apparaît donc clairement que le présent décret a étendu le champ matériel des données pouvant être recueillies, que cet élargissement empiète sur la délimitation voulue par le législateur entre « *métadonnées* » et « *contenu* » et pourrait même nécessiter techniquement la mise en œuvre de techniques de *deep packet inspection* à laquelle le gouvernement, pour justifier l'adoption du texte, s'était pourtant opposé — à raison — du fait de l'atteinte qu'elle porte à la confidentialité des communications et au secret des correspondances.

En étendant le champ matériel des données pouvant être recueillies au-delà de la délimitation stricte des « *informations ou documents* » figurant à l'article L. 851-1 du code de la sécurité intérieure (tel

qu'interprété par le Conseil constitutionnel), le décret attaqué a ainsi été pris par une autorité incompétente en ce qu'il contient des dispositions relevant exclusivement de la compétence du législateur.

*Sur les différents types d'accès aux données de connexion*

**VI-2.2 Deuxièmement**, si le législateur a prévu plusieurs types d'accès à ces « *informations ou documents* », il n'en demeure pas moins que le champ des données de connexion pouvant être collectées par l'autorité administrative ne varie aucunement en fonction du type d'accès. Ainsi, en matière d'accès en temps réel, l'article L. 851-2 ne permet que le recueil *« des informations ou documents mentionnés au même article L. 851-1 »*. De même, concernant la détection automatisée, l'article L. 851-3 précise à l'alinéa I que *« ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1 »*.

En somme, il n'existe dans le texte de loi qu'une seule notion d'« *informations ou documents* » auxquels il peut être accédé à des fins de renseignement. Cette notion est délimitée à l'article L. 851-1 CSI, mais elle vaut également pour l'article L. 851-2 — le Conseil constitutionnel en a donné une interprétation uniforme pour les deux articles (voir *infra*, les articles visés dans le considérant 55 de la décision Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC).

Compte-tenu de la formulation de l'article L. 851-3, le champ des données doit être encore plus restreint ; celui-ci disposant, au surplus, ne pas pouvoir « *permettre l'identification des personnes auxquelles les informations ou documents se rapportent*. »

Par conséquent, toute donnée exclue du champ de l'article L. 851-1 est également exclue du champ des articles L. 851-2 et, *a fortiori*, L. 851-3.

*Sur la délimitation du champ des données auxquelles il peut être accédé*

**VI-2.3 Troisièmement**, le Conseil constitutionnel a pu expliciter la délimitation du champ des données auxquelles il peut être accédé en considérant que :

« *L'autorisation de recueil de renseignement prévue par les articles L. 851-1 et L. 851-2 porte uniquement sur les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes mentionnées au considérant 52 ; que selon les dispositions du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées par les opérateurs de communications électroniques et les personnes offrant au public une connexion permettant une telle communication portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent 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 ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées par les personnes offrant un accès à des services de communication en ligne et celles assurant le stockage de diverses informations pour mise à disposition du public par ces services sont celles 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 ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées* » (Conseil constit., 23 juill. 2015, Loi renseignement, 2015-713 DC, cons. 55).

La notion des données de connexion des articles L. 851-1 et L. 851-2 recouvre donc :

- « *Les données conservées et traitées par les opérateurs de communications électroniques […]* » au titre du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) et qui « *portent exclusivement sur*

*l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* » ;

- « *Les données conservées par les personnes offrant un accès à des services de communication en ligne et celles assurant le stockage de diverses informations pour mise à disposition du public par ces services » au titre du paragraphe II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et qui sont « 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* ».

Dès lors, il apparaît clairement que la notion de données de connexion des articles L. 851-1 à L. 851-3 s'inscrit **dans le cadre de la délimitation des données conservées**, d'un côté, par les opérateurs de communications électroniques et, de l'autre côté, par les prestataires de services de communication au public en ligne (eux-mêmes répartis entre fournisseurs d'accès et hébergeurs). Dans sa décision précitée, le Conseil constitutionnel a ainsi entendu circonscrire le champ matériel des données de connexion en le rattachant au cadre juridique préexistant relatif à la conservation des données de connexion.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) considère d'ailleurs, en ce sens, qu'en application de l'article L. 851-1, les données de connexion susceptibles d'être recueillies « *ne peuvent être **que des données préalablement conservées** par les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet* » (CNCTR, délibération n° 1/2016 du 14 janvier 2016).

Le cadre juridique de la conservation des données de connexion se distingue généralement en deux régimes. Le régime applicable aux opérateurs de communications électroniques, encadré par le CPCE, et le régime applicable aux prestataires de services de communication au public en ligne, encadré par l'article 6, alinéa II, de la LCEN; étant précisé que les données de connexion « ***ne peuvent porter sur le contenu de correspondances ou les informations consultées*** » (*in fine*,

considérant 55 de la décision Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC).

*Sur le régime des données de connexion applicable aux opérateurs de communications électroniques*

**VI-2.4 Quatrièmement**, le régime des données de connexion applicable aux opérateurs de communications électroniques figure à l'article L. 34-1 CPCE et est applicable aux « *données relatives au trafic* », c'est-à-dire, « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* » (article L. 32 CPCE).

L'article L. 34-1 CPCE pose, tout d'abord, le principe de l'effacement ou de l'anonymisation des données relatives au trafic :

« *II.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI. […]* »

Par exception à ce principe d'effacement ou d'anonymisation, l'article L. 34-1, III, dispose que « *pour certaines catégories de données techniques* », il peut être prévu de « *différer pour une durée maximale d'un an* » l'effacement ou l'anonymisation, dans les limites fixées par le paragraphe VI (visé explicitement par le Conseil constitutionnel dans sa décision précitée):

« *III.-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. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.* »
[…]

« *VI.-Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux*.

« *Elles ne peuvent 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*. »

Par conséquent, les données de connexion des opérateurs de communications électroniques ne concernent que :

- « *Certaines catégories de données techniques » et non l'ensemble des données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques, lesquelles doivent donc être par principe effacées ou anonymisées;*

- Les données « *conservées et traitées* » exceptionnellement et qui portent « *exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* » — à l'exclusion du « *contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications*. »

*Sur le régime des données de connexion applicable aux prestataires de services de communication au public en ligne*

**VI-2.5 Cinquièmement**, le régime des données de connexion applicable aux prestataires de services de communication au public en ligne, figurant au paragraphe II de l'article 6 de la LCEN, est applicable aux « *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*. »

*Sur la notion des données de connexion aux fins de renseignement*

**VI-2.6 Sixièmement**, le champ matériel des données de connexion auxquelles il peut être accédé (les « *informations ou documents* » de l'article L. 851-1 CSI) pour des finalités relatives au renseignement est donc la juxtaposition, d'une part, du régime des données de connexion applicable aux opérateurs de communications électroniques et, d'autre part, du régime des données de connexion applicable aux prestataires de services de communication au public en ligne.

Est donc exclue du périmètre des « *informations ou documents* » de l'article L. 851-1, de l'article L. 851-2 (et *a fortiori* L. 851-3), toute donnée technique accédée sur un réseau de communications électroniques ou sur un service de communication au public en ligne et qui sortirait respectivement, soit du champ des catégories de données techniques faisant exceptionnellement l'objet d'une conservation d'un an, soit du champ des données de nature à identifier un contributeur de contenu en ligne.

Or, le décret attaqué contient dans la liste des données de connexion, des informations ou documents qui sortent du périmètre ainsi fixé par le législateur.

**En l'espèce,** l'article 2, 3°, du décret 2016-67 dispose :

*« Après l'article R. 851-4, il est créé une section 2 et une section 3 ainsi rédigées :*

*« Section 2*
*« Données de connexion susceptibles d'être recueillies*

*« Art. R. 851-5.-I.-Les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées :*
*« 1° Ceux énumérés aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 modifié 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 ;*
*« 2° Les données techniques autres que celles mentionnées au 1° :*
*« a) Permettant de localiser les équipements terminaux ;*
*« b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;*
*« c) Relatives à l'acheminement des communications électroniques par les réseaux ;*
*« d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;*
*« e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.*
*« II.-Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé.*
*« Les informations énumérées au 2° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3 dans les conditions et limites prévues par ces articles et sous réserve de l'application de l'article R. 851-9. […] »*

Les dispositions citées dans le paragraphe 1° de l'article R. 851-5 ci-dessus, à savoir les articles R. 10-13, R. 10-14 (CPCE) et l'article 1er du décret n° 2011-219, correspondent aux données relevant du périmètre des données de connexion du paragraphe VI de l'article L. 34-1 CPCE et du paragraphe II de l'article 6 LCEN — conformément à l'interprétation donnée par le Conseil constitutionnel précitée.

En revanche, les autres dispositions de l'article R. 851-5 vont au-delà de ce périmètre des données de connexion.

**D'abord**, la distinction opérée au paragraphe II de l'article R. 851-5 entre (i) les données de connexion pouvant être recueillies en différé, (ii) les données de connexion pouvant être recueillies en temps réel et (iii) les données analysées par détection automatique, méconnaît les

dispositions législatives du code de la sécurité intérieures, lesquelles ne prévoient aucunement qu'il puisse y avoir différents champs de données de connexion selon le type d'accès — à l'inverse, le législateur a prévu que seules les « *informations ou documents* » de l'article L. 851-1 pouvaient être recueillies, que ce soit au titre de l'article L. 851-1, ou au titre des articles L. 851-2 et L. 851-3, lesquels renvoient explicitement au premier, c'est-à-dire à l'article L. 851-1 (pour lequel la CNCTR considère d'ailleurs qu'il ne peut concerner « ***que des données préalablement conservées*** *par les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet* » comme indiqué *supra*).

Cette interprétation est confirmée sans équivoque par le Conseil constitutionnel, qui procède à une analyse commune du champ des informations relevant des articles L. 851-1 et L. 851-2 (considérant 55 précité).

Partant, le décret apparaît contraire aux dispositions des articles L. 851-1 à L. 851-3.

**Ensuite**, l'article R. 851-5, I, 2° étend la liste des données de connexion mais, à l'inverse du point 1°, créé un régime unique applicable à l'ensemble des prestataires concernés sans distinctions.

Par les dispositions du CPCE et celles de la LCEN, le législateur a pourtant associé un régime de conservation différentié entre les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs. Or, si le décret 2016-67 suit cette distinction de régimes au point 1° de l'article R. 851-5.-I qu'il créé, le décret attaqué la méconnaît au point 2°.

Le point 2° du paragraphe I de l'article R. 851-1 applique donc un régime unique à des prestataires techniques relevant de régimes différents. Or, ce choix du pouvoir règlementaire est critiquable et contraire aux objectifs de lisibilité et d'intelligibilité, mais aussi de sécurité juridique, car le décret a pour effet de créer une grande confusion pour les prestataires concernés. Cette confusion avait bien été relevée par l'ARCEP, dans son avis sur le projet de décret en question, n° 2016-0025 du 14 janvier 2016, lequel énonçait que :

*« afin de lever les incertitudes, l'ARCEP estime qu'il serait souhaitable que le projet de décret distingue, parmi les catégories d'informations ou de documents, mentionnées au nouvel article R. 851-5,* ***celles qui peuvent être recueillies auprès de chacune des trois catégories d'acteurs concernés.*** *De même, l'ARCEP invite le Gouvernement à définir précisément la nature des informations ou documents en cause. »*

De plus, dans la délibération n° 2015-455 du 17 décembre 2015, la CNIL procédait au même constat et relevait que :

*« si l'énumération prévue aux 2° à 6° du projet d'article R. 851-1 du CSI est de nature à préciser les informations ou documents recueillis, elle* ***ne donne pas de définition précise des données pouvant être recueillies au titre de chaque catégorie****, alors même que les opérateurs et personnes visées aux 1° et 2° de l'article 6 de la loi du 21 juin 2004 sont pénalement responsables sur la base des articles L.39-3 CPCE et 6 VI de la loi du 21 juin 2004. Il importe dès lors que ceux-ci puissent connaître avec précision l'étendue de leurs obligations de conservation et d'effacement. »*

Force est de constater que le pouvoir réglementaire n'en a aucunement tenu compte. Ce faisant, le décret attaqué crée, d'une part, un amalgame entre les régimes et, d'autre part, une confusion sur la nature précise des informations ou documents en cause.

La Commission nationale de contrôle des techniques de renseignement, qui a tenté une explication technique de chaque catégorie de données, émet d'ailleurs une réserve importante dans son avis concernant l'analyse technique à laquelle elle a procédé :

*« les développements ci-dessus sur la nature des données de connexion constituent une analyse globale, empirique,* ***non exhaustive et non définitive****. Cette analyse a* ***vocation à être approfondie****, en particulier lors de la rédaction de l'arrêté tarifaire prévu au nouvel article R. 873-2 du code de la sécurité intérieure, qui doit énumérer les prestations pouvant être demandées aux opérateurs de communications électroniques, aux hébergeurs et aux fournisseurs de services sur internet pour recueillir les données de connexion. La CNCTR révisera en outre périodiquement l'analyse en fonction des évolutions techniques. Elle demande en conséquence que les nouveaux types de*

*données qui pourraient être regardées comme faisant partie des données de connexion fassent l'objet d'un avis de sa part avant toute autorisation de recueil, afin qu'elle puisse s'assurer qu'aucun contenu de communications ne sera collecté. »*

Il convient de préciser qu'il n'existe, à notre connaissance, aucune trace de cette révision périodique et que l'arrêté tarifaire annoncé n'a toujours pas été publié. En outre, l'association requérante French Data Network a envoyé le 12 octobre une demande d'accès auprès de la CNCTR, sur le fondement du code des relations entre le public et l'administration, pour obtenir tout avis portant sur les nouveaux types de données techniques.

Si le Conseil d'État souhaite approfondir l'analyse des catégories de données du décret afin de déterminer leur teneur, les associations requérantes l'invitent à avoir recours à une expertise sur ce point particulier conformément à l'article R. 621-1 du code de justice administrative.

**Enfin**, en ne créant pas des régimes d'accès aux données de connexion distincts selon les prestataires concernés, le point 2° du paragraphe I de l'article R. 851-1 permet d'englober des données allant au-delà de la notion d'« *informations ou documents* » telle que définie à l'article L. 851-1 et telle qu'applicable à l'article L. 851-2 (et *a fortiori* L. 851-3), lue à la lumière de l'interprétation donnée par le Conseil constitutionnel.

À titre liminaire, observons que même si le paragraphe I de l'article R. 851-5.-I. créé par le décret prévoit bien d'exclure le « *contenu des correspondances échangées ou des informations consultées* », ce dernier liste pour autant des données qui relèvent, pour certaines, de contenu des correspondances ou des informations consultées. C'est le cas, notamment, des « *informations consultées* » par l'utilisateur d'un service de communication électronique (L. 34-1 CPCE) ou par l'abonné d'un service d'accès à des services communication au public en ligne (paragraphe 1 du I de l'article 6 LCEN).

Par ailleurs, dans son avis n° 2016-0025 du 14 janvier 2016 sur le projet de décret (p. 3 et 4), l'ARCEP relevait déjà à cet égard qu'« *il pourrait être délicat pour les opérateurs de communications électroniques, de déterminer de manière suffisamment certaine, parmi les catégories*

*d'informations ou de documents définies au nouvel article R. 851-5 du CSI (3° de l'article 2 du projet de décret), celles qui sont couvertes par le secret des correspondances ou portent sur des informations consultées au sens de l'article L. 34-1 du CPCE*. »

Pour cause, les catégories de données du point 2° du paragraphe I de l'article R. 851-5 mêlent en effet des données de trafic avec des données de contenu ou des informations échangées.

*Sur les données techniques « relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne »*

**VI-2.7 Septièmement**, le décret attaqué permet de recueillir 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 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 :

*« 2° Les données techniques autres que celles mentionnées au 1° [énumérées aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011]:*
*[…]*
*« b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ; »*

Le décret permet ainsi d'accéder aux données « *relatives à l'accès des équipements terminaux […] aux services de communication au public en ligne* » auprès d'un opérateur.

Dans sa délibération n° 1/2016 du 14 janvier 2016, la CNCTR indique que ces données :

*« peuvent être des données techniques envoyées par un équipement terminal pour manifester son existence à un réseau ou à un service en ligne afin d'établir une connexion. Par exemple, lorsqu'un utilisateur désactive le mode avion de son smartphone après un atterrissage, son*

*équipement émet des signaux afin d'accéder aux réseaux présents dans son environnement. »*

Cet exemple est, toutefois, loin d'être représentatif de l'ensemble des données concernées par cette définition. En effet, cette catégorie est bien plus large et comprend des informations échangées ou des informations révélant le contenu d'une communication.

En effet, les adresses URL font également partie de cette catégorie. Les URL sont des adresses électroniques permettant de localiser un contenu; il convient de les différentier des adresses IP qui, elles, permettent de localiser une machine sur un réseau pour acheminer une communication.

Une URL permet l'accès d'un terminal à un service de communication au public en ligne. Par exemple, l'URL http://www.conseil-etat.fr/Conseil-d-Etat/Contacts-Informations-pratiques permet à un logiciel de navigation de contenus sur Internet de former une requête à destination d'un serveur (par exemple, les machines du prestataire technique du Conseil d'État) afin que ce serveur lui réponde et envoie le contenu demandé.

Cette information sera donc échangée entre l'équipement terminal de l'utilisateur, d'une part, et le service de communication au public en ligne d'autre part.

Du point de vue des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 CPCE ainsi que des personnes mentionnées au paragraphe 1 du I de l'article 6 de la LCEN, l'adresse URL n'est pas une donnée « *nécessaire à l'acheminement de la communication* », contrairement à l'adresse IP (NB : Dans la plupart des configurations d'accès à Internet – à l'exception de certains réseaux, notamment des réseaux d'entreprise ayant recours à des proxys ou d'autres systèmes complexes –, l'URL n'est même pas traitée par le réseau de l'opérateur. Un fournisseur d'accès à Internet a uniquement besoin d'acheminer le paquet à une adresse IP – l'adresse d'une machine connectée au réseau – mais n'a aucunement besoin de l'adresse URL, qui correspond à l'adresse d'un contenu stocké sur une machine).

Mais l'adresse URL constitue bien une information consultée et une information échangée, entre le terminal de l'abonné et un service de communication au public en ligne.

C'est d'ailleurs pourquoi l'URL constitue une donnée susceptible de fournir des informations sur le contenu consulté, comme le relève la CNIL, dans sa délibération n° 2015-455 du 17 décembre 2015 portant sur le projet de décret :

*« L'URL étant porteuse par nature des informations consultées, elle ne saurait être conservée par les opérateurs au-delà du temps nécessaire à l'acheminement de la communication. »*

À cet égard, il convient de relever comme expliqué *supra* que l'URL n'est pas *nécessaire* à l'acheminement de la communication, cette donnée n'étant d'ailleurs pas traitée par les réseaux des opérateurs et FAI comme l'association requérante French Data Network ou les membres de la Fédération des fournisseurs d'accès Internet associatifs.

En incluant dans les données recueillies auprès des opérateurs, les données relatives à l'accès des équipements terminaux aux services de communication au public en ligne, le décret y inclue principalement — si ce n'est exclusivement — des informations échangées ainsi que des informations révélant les contenus consultés, comme l'URL.

*Sur les données techniques « relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne »*

**VI-2.8 Huitièmement**, le décret attaqué permet de recueillir 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 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 :

*« 2° Les données techniques autres que celles mentionnées au 1° [énumérées aux articles R. 10-13 et R. 10-14 du code des postes et des*

*communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011]:*
*[…]*
*« d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ; »*

Le décret permet ainsi d'accéder aux données « *relatives à l'identification et à l'authentification d'un utilisateur […] d'un service de communication au public en ligne* » auprès d'un opérateur.

Dans sa délibération n° 1/2016 du 14 janvier 2016, la CNCTR indique que ces données incluent « *les login et mots de passe des personnes* ».

Or, un « *service de communication au public en ligne* » est défini à l'article 1, IV, de la LCEN. Il s'agit d'un service de « *transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur.* »

Par définition, l'identification et l'authentification d'un utilisateur d'un service de communication au public en ligne implique *de facto* l'échange réciproque d'informations entre émetteur et récepteur, de telles sorte que le recueil de données relatives à un service de communication au public en ligne constitue le recueil d'informations échangées — lesquelles sont exclues du périmètre des données tel qu'interprété par le Conseil constitutionnel pour les articles L. 851-1 et L. 851-2.

Ces données d'identification et d'authentification comprennent donc des « *informations consultées* », auxquelles les opérateurs (notamment fournisseurs d'accès Internet) ne sauraient donner accès, sauf à contredire les termes de la loi et à déployer des moyens disproportionnés tels que des technologies de *deep packet inspection*.

*Sur les données techniques « relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels »*

**VI-2.9 Neuvièmement**, le décret attaqué permet de recueillir 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 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 :

*« 2° Les données techniques autres que celles mentionnées au 1° [énumérées aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011]:*
*[…]*
*« e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels. »*

Cette formulation manque d'intelligibilité et, en conséquence, laisse une marge considérable d'interprétation.

Dans sa délibération n° 1/2016 du 14 janvier 2016, la CNCTR explique que ces données :

*« Désignent **notamment** des informations émises par un smartphone sans que son utilisateur le demande, telle celles relatives à leurs paramètres d'affichage (taille d'écran, format audio, capacités de mémoire, type de système d'exploitation, liste des applications et numéros de version ».*

De même que pour les catégories de données précédentes, de telles données ne sont nullement nécessaires à l'acheminement des communications et font en réalité partie d'informations échangées par le logiciel exécuté sur un terminal d'une part et un service de communication en ligne d'autre part. Par conséquent, en tant qu'informations échangées, ces données ne sauraient être recueillies auprès des opérateurs ou des fournisseurs d'accès à Internet et, de plus,

le recueil de telles informations nécessiterait fort probablement la mise en place de techniques de *deep packet inspection*.

*Sur les données techniques « relatives à l'acheminement des communications électroniques par les réseaux »*

**VI-2.10 Dixièmement**, le décret attaqué permet de recueillir 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 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 :

*« 2° Les données techniques autres que celles mentionnées au 1° [énumérées aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011]:*
*[…]*
*« c) Relatives à l'acheminement des communications électroniques par les réseaux ; »*

Les articles R. 10-13 et R. 10-14 contiennent une liste de « données techniques » qui constituent des données relatives au trafic, soit des données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques (L. 32 CPCE).

Par le truchement du point 1° et du point 2° c), le décret attaqué permet de recueillir toutes les données relatives à l'acheminement des communications électroniques par les réseaux.

Or, comme exposé *supra*, en droit, l'article L. 34-1, paragraphe II, pose le principe de l'effacement des données relatives à l'acheminement des communications électroniques par les réseaux (sauf exception, prévue notamment au paragraphe III du même article).

De cette manière, le décret attaqué a pour effet de renverser l'exception et le principe, allant ainsi directement à l'encontre de ce que prévoit le législateur.

**VI-3 Il résulte de tout ce qui précède** qu'en permettant à l'autorité administrative le recueil en temps réel ou par détection automatique de données techniques autres que les seuls « *informations ou documents* » prévus à l'article L. 851-1, le pouvoir réglementaire a méconnu l'étendue de sa compétence.

Cette méconnaissance a pour conséquence l'élargissement indu des obligations des opérateurs et, dès lors, viole le droit au respect de la vie privée dont découlent tant le principe de confidentialité des communications électroniques que le droit au secret des correspondances.

Pour cette raison, le dispositions réglementaires litigieuses, et en particulier le 2° du I et le II de l'article R. 851-5 du code de la sécurité intérieure sont vouées à la censure.

**PAR CES MOTIFS**, et tous autres à produire, déduire, suppléer, au besoin même d'office, les associations exposantes persistent dans les conclusions de leurs précédentes écritures.

SPINOSI & SUREAU
SCP d'Avocat au Conseil d'État et à la Cour de cassation