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

MEMOIRE EN REPLIQUE

EN VUE DE L'AUDIENCE DU 11 JUILLET 2018 A 14H

POUR : **French Data Network (Réseau de données français), dite FDN**

La Quadrature du Net

Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN (FFDN)

SCP SPINOSI & SUREAU, avocat au conseil d'État

CONTRE : 1/ Le Premier ministre

2/ Le ministre de l'intérieur

Sur la requête n° 397.851

I. À la suite du dépôt par le Premier ministre et le ministère de l'intérieur d'observations en défense, les associations French Data Network (FDN) et La Quadrature du Net ainsi que la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) entendent formuler les observations complémentaires suivantes.

Persistant dans l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures, les exposantes entendent réfuter l'argumentation présentée par le Premier ministre et le ministère de l'intérieur dans leur mémoire.

Sur le champ d'application de l'arrêt Tele2 Sverige

II. En premier lieu, le Premier ministre prétend dans ses observations que **l'arrêt *Tele2 Sverige*** rendu par la Cour de justice le 21 décembre 2016 ne saurait être opposé aux dispositions visées par la présente affaire (CJUE, G.C., 21 déc. 2016, *Tele2 Sverige et al*., Aff. C-203/15 et C-698/15)

À titre liminaire, il est important de noter que, pour ce faire, le Premier ministre a abandonné l'argumentation qu'il avait précédemment développée afin d'écarter l'applicabilité de la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte ») aux dispositions en cause (voir par exemple à partir de la page 3 de son mémoire en défense du 4 juillet 2016 dans l'affaire n° 397.851).

Reprenant désormais le raisonnement des requérantes, le Premier ministre reconnaît que, « *bien qu'il appartienne aux États membres d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure,* ***le seul fait qu'une décision concerne la sûreté de l'État ne saurait entraîner l'inapplicabilité du droit de l'Union*** ».

Désormais, le Premier ministre tente de faire valoir que « *la solution retenue par la Cour de justice dans l'arrêt Tele2 Sverige ne saurait être transposée aux traitements de données visant exclusivement la sécurité publique, la défense et la sûreté de l'Etat* » en ce que cet arrêt ne concernerait que « *la lutte contre la criminalité* » et que la Cour

n'aurait pas été compétente pour retenir une solution identique au regard de ces autres finalités.

Mais ces deux arguments sont parfaitement infondés.

II-1 D'emblée, le Premier ministre se méprend en opposant la finalité de « *sécurité publique* » à celle de « *lutte contre la criminalité* » qui, en droit de l'Union, se confondent.

En effet, il suffit de lire le premier article de la directive (UE) 2016/680 – pourtant invoquée par le Premier ministre – pour s'en convaincre.

Cet article précise que « *la présente directive établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à* ***des fins de prévention et de détection des infractions pénales****, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales,* ***y compris la protection contre les menaces pour la sécurité publique*** *et la prévention de telles menaces* ».

La « *lutte contre les infractions pénales* », qui est précisément l'objet de l'arrêt *Tele2*, est explicitement définie en droit de l'Union comme comprenant la sauvegarde de la « *sécurité publique* », que le Premier ministre prétend, à tort donc, étrangère à ce même arrêt.

II-2 Une telle erreur révèle une méprise plus générale sur les **compétences législatives de l'Union**, que le Premier ministre prétend étrangères aux finalités que les mesures visées par la présente affaire poursuivent.

Pour dissiper cette méprise, l'évolution des compétences législatives de l'Union en la matière depuis vingt ans doit être brièvement rappelée.

II-2.1 Au 1er mai 1999, dans sa version révisée par le traité d'Amsterdam, le Traité sur l'Union européenne (TUE) prévoyait à son article K.1 que, « *sans préjudice des compétences de la Communauté*

européenne, l'objectif de l'Union est d'offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice, en élaborant une ***action en commun*** *entre les États membres dans le domaine de la coopération policière et judiciaire* ***en matière pénale*** ».

L'article K.3 du TUE ajoutait que « *l'action en commun dans le domaine de la coopération judiciaire en matière pénale vise, entre autres à [...] adopter progressivement des mesures instaurant des règles minimales relatives aux éléments constitutifs des infractions pénales et aux sanctions applicables dans les domaines de la* ***criminalité organisée****, du* ***terrorisme*** *et du trafic de drogue* ».

Toutefois, cette action en commun ne pouvait être réalisée que dans un cadre spécifique et limité.

En ce sens, l'article K.6, §2, du TUE prévoyait que, en matière pénale, seul « *le Conseil [...] peut, statuant à l'unanimité à l'initiative de tout État membre ou de la Commission: [...] arrêter des* ***décisions-cadres*** *aux fins du* ***rapprochement*** *des dispositions législatives et réglementaires des États membres. Les décisions-cadres lient les États membres quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. Elles ne peuvent entraîner d'effet direct* ».

Il est à noter que le traité de Nice, entré en vigueur le 1er février 2003, n'a pas altéré ces dispositions, lesquelles ont seulement fait l'objet d'une renumérotation aux articles 29, 31 et 34 du TUE, où elles sont restées inchangées jusqu'au 1er décembre 2009.

Le cœur de la présente affaire concerne la directive 2002/58/CE qui, adoptée le 12 juillet 2002, pose le cadre européen de la conservation et de l'utilisation des données de connexion.

Cette directive n'est pas une décision-cadre : au moment de son adoption, elle ne pouvait donc pas opérer à elle-seule un « *rapprochement des dispositions législatives et réglementaires des États membres* » en matière pénale ou de sécurité.

Ainsi, elle précisait à son article 1er, §3 que :

« *La présente directive ne s'applique pas aux activités* ***qui ne relèvent pas du Traité instituant la Communauté européenne****, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* ».

En effet, ces activités « *ne relèvent pas du traité instituant la Communauté européenne* » car, à l'époque, comme expliqué ci-avant, elles ne relevaient que du TUE.

II-2.2 Après l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, ces distinctions ont disparu.

L'article 67, §3, du traité sur le fonctionnement de l'Union européenne (TFUE) prévoit que « *l'Union œuvre pour assurer un niveau élevé de sécurité par des mesures de prévention de la criminalité [...] et, si nécessaire, par le rapprochement des législations pénales* ».

Ce rapprochement ne passe maintenant plus par des décisions-cadres du Conseil mais, au contraire, par des directives ordinaires de l'Union.

L'article 83, §1, du TFUE prévoit désormais que « *le Parlement européen et le Conseil, statuant* ***par voie de directives*** *conformément à la procédure législative ordinaire, peuvent établir des règles* » dans les domaines suivants : « *le* ***terrorisme****, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la* ***criminalité organisée*** » .

Par ailleurs, l'article 16, §2, du TFUE prévoit que « *le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du* ***traitement des données à caractère personnel*** *par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union* ».

Ainsi, depuis le 1er décembre 2009, les traitements de données personnelles réalisés à des fins de sécurité publique ou de lutte contre la criminalité sont entièrement entrés dans le champ des compétences législatives l'Union.

C'est pour cela que la directive 2016/680 prévoit désormais – contrairement aux directives antérieures à 2009 – qu'elle s'applique en matière criminelle et de sécurité publique.

II-3 Concrètement, les dispositions nationales concernées par la présente affaire entrent manifestement dans le champ des compétences législatives de l'Union.

II-3.1 Premièrement, le régime français de conservation généralisée des données de connexion poursuit des finalités qui, notamment listées à l'article L34-1 du CPCE, recoupent largement les compétences législatives de l'Union.

Parmi les recoupements les plus manifestes, peuvent être cités la protection du **droit d'auteur** (voir par exemple la directive 2001/29 sur l'harmonisation des règles de protection du droit d'auteur), la **cybersécurité** (voir par exemple la directive 2016/1148 « *destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information* ») ou la lutte contre la **criminalité** (voir par exemple la directive 2016/680 précitée).

II-3.2 Deuxièmement, l'accès par les services de renseignement aux données ainsi conservées n'est autorisé que pour des finalités qui, listées à l'article L811-3 du code de la sécurité intérieure (ci-après « CSI »), recoupent elles-aussi largement les compétences législatives de l'Union.

Parmi les recoupements les plus manifestes, peuvent être cités l'exécution des **engagements européens**, la prévention de la **criminalité** et de la délinquance organisées et la prévention du **terrorisme**.

À ce dernier titre, l'Union européenne, compétente depuis 2009 pour prendre des actes législatifs en la matière, a adopté une **directive 2017/541** « relative à la lutte contre le terrorisme », qui « *énumère de manière exhaustive un certain nombre d'**infractions graves**, telles que les atteintes à la vie d'une personne, en tant qu'actes intentionnels pouvant être qualifiés d'**infractions terroristes*** » (considérant 8).

Cette directive révèle ici clairement qu'en droit de l'Union, le terrorisme est une « *infraction grave* » et que l'arrêt ***Tele2*** **couvre donc déjà** les dispositions nationales prises pour lutter contre cette menace.

La Cour de justice le précise d'ailleurs explicitement dans cet arrêt *Tele2*, en évoquant « *l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme* » (précité, § 103).

II-3.3 Troisièmement, il faut rappeler que la notion de « *lutte contre la criminalité* » ne se résume pas aux seules activités **répressives** mais couvre aussi les activités **préventives** poursuivies par les services de renseignement.

L'arrêt *Tele2* a ainsi été rendu au regard d'une loi britannique qui prévoyait de conserver des données auxquelles il ne pouvait être accédé qu'à « *des fins de prévention ou de détection de la criminalité* » et non à des fins de répression (§ 33 de l'arrêt). En outre, le même arrêt a aussi été rendu au regard d'une loi suédoise qui prévoyait des finalités à la fois préventives et répressives, visant à « *prévenir, empêcher ou constater une activité criminelle* » (§ 22 de l'arrêt).

II-4 Seules échappent encore à la compétence législative de l'Union les questions propres à la « ***sécurité nationale*** ».

Or, le droit de l'Union définit trois catégories de finalités relatives à la « *sécurité* ».

Premièrement, la « ***sécurité publique*** », telle qu'expliquée ci-avant, couvre les questions de sécurité pour lesquelles l'Union et les États membres peuvent légiférer.

Deuxièmement, la « ***politique étrangère et de sécurité commune*** », adressée au titre V, chapitre 2, du TUE, concerne la sécurité extérieure de l'Union-même, que celle-ci peut seulement coordonner et à propos de laquelle ni l'Union ni les État membres ne peuvent légiférer.

Troisièmement, et en creux, la « ***sécurité nationale*** » couvre toutes les questions de sécurité échappant au champ de ces deux premières catégories. Le Traité sur l'Union précise à son article 4, §2, que « *la sécurité nationale reste de la seule responsabilité de chaque État membre* ».

Cette répartition est parfaitement décrite par la directive 2016/680 qui, s'appliquant en matière de « *sécurité publique* », précise que :

« *Etant donné que la présente directive ne devrait pas s'appliquer au traitement de données à caractère personnel effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union, il convient que les activités relatives à la* ***sécurité nationale****, les activités des agences ou des services responsables des questions de* ***sécurité nationale*** *et le traitement de données à caractère personnel par les États membres dans le cadre d'activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne [qui concerne la* ***politique étrangère et de sécurité commune****] ne soient pas considérées comme des activités relevant du champ d'application de la présente directive* » (Cons. 14).

II-5 Concrètement, la sécurité nationale n'est qu'une **finalité minoritaire** parmi celles que poursuivent les services de renseignement français.

Dans son 23ème et dernier rapport, la Commission nationale de contrôle des interceptions de sécurité (ci-après « CNCIS ») précise que, en matière d'interceptions de sécurité, « *entre le 1er janvier et le 30 avril 2015, [...] la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 48%, suivie de la prévention du terrorisme avec 38% (en augmentation de 12 points par rapport à la moyenne 2014) et de* ***la sécurité nationale avec 12%*** ».

Certes, ni la CNCIS ni la commission nationale de contrôle des techniques de renseignement (ci-après « CNCTR ») n'ont hélas encore donné de chiffres quant à la répartition des finalités poursuivies en matière d'accès aux données de connexion.

Il semble toutefois improbable que cette répartition soit sensiblement différente de celle décrite en matière d'interceptions de sécurité.

Ainsi, environ **86 % des accès** aux données de connexion par les services français se feraient pour des finalités de lutte contre la criminalité (organisée ou terroriste) et **doivent donc déjà respecter les solutions retenues par l'arrêt *Tele2***.

Un dixième seulement des activités de renseignement sont étrangères au champ des compétences législatives de l'Union – ce qui, d'après le Premier ministre, devrait les isoler des solutions retenues par cet arrêt *Tele2*.

Or, à supposer même qu'il soit possible un instant – pour les seuls besoins de la démonstration – de retenir cette conclusion, il serait de toute façon injustifiable de ne pas appliquer les solutions retenues par l'arrêt *Tele2* à la majorité des activités de renseignement au seul prétexte qu'une minorité d'entre elles y échapperaient.

II-6 De plus, et en toute hypothèse, les activités propres à la **sécurité nationale** doivent elles-aussi respecter les solutions retenues par l'arrêt *Tele2*.

En effet, ces activités doivent respecter **la Charte**, et c'est en application de celle-ci que ces solutions ont été imposées.

II-6.1 L'article 51, §1, de la Charte prévoit que ses dispositions s'imposent aux États membres « *lorsqu'ils mettent en œuvre le droit de l'Union* ».

La notion de « *mise en œuvre* » du droit de l'Union est le cœur du débat.

De la façon la plus évidente, un État membre « *met en œuvre* » le droit de l'Union lorsqu'il transpose une directive dans son droit national – en l'espèce, en limitant les conditions de conservation et d'utilisation des données de connexion, tel qu'exigé par la directive 2002/58.

De même, un État membre « *met en œuvre* » le droit de l'Union lorsque, ayant transposé une directive, il intègre dans son droit national des mesures prises en application d'une dérogation prévue par cette même directive – en l'espèce, en prévoyant un régime de conservation généralisée à des fins de police judiciaire et administrative.

Dans ce dernier cas, il **« *met en œuvre* » une dérogation** prévue par le droit de l'Union et ainsi **« *met en œuvre le droit de l'Union* »** lui-même.

Ce raisonnement a notamment été explicité par la Cour de justice dans son arrêt *Pfleger* (C-390/12) du 30 avril 2014, point 36 :

« **L'emploi, par un État membre, d'exceptions prévues par le droit de l'Union** pour justifier une entrave à une liberté fondamentale garantie par le traité doit, dès lors, être considéré, ainsi que Mme l'avocat général l'a relevé au point 46 de ses conclusions, comme **«mettant en œuvre le droit de l'Union»**, au sens de l'article 51, paragraphe 1, de la Charte. »

II-6.2 C'est un tel raisonnement qu'a suivi la Cour de justice dans son arrêt *Tele2*.

Comme précédemment exposé, au moment de son adoption, la directive 2002/58 ne pouvait prévoir de règles spécifiques en matière pénale ou de sécurité nationale, et elle le rappelait à son article 1, §3.

La directive prévoyait des règles générales en matière de secret des correspondances, ainsi que, à son article 15, des dérogations spécifiques à ces règles, notamment en matière pénale et de sécurité nationale.

De plus, elle exigeait à ce même article que ces dérogations respectent un **principe de proportionnalité**, que l'on retrouve aujourd'hui aussi à l'article 52, §1, de la Charte.

Dans son arrêt *Tele2*, en substance, la Cour de justice considère que la « *mise en œuvre* » des dérogations prévues par la directive constitue une « *mise en œuvre du droit de l'Union* », de sorte que la Charte s'applique aux mesures nationales qui bénéficient de ces dérogations.

En effet, au point 73 de sa décision, la Cour considère que l'article 15 de la directive, qui exige la même proportionnalité que celle exigée par la Charte, **s'applique à toutes « *les mesures nationales qui y sont visées* »**.

Et ce, alors même que ces mesures poursuivent des finalités exclues à l'article 1, §3, de la directive, qu'il s'agisse de mesures luttant contre la criminalité (explicitement introduites par un « telles que ») ou poursuivant les autres finalités visées à l'article 15, dont la sécurité nationale.

Le Premier ministre se méprend donc manifestement quand il prétend que l'arrêt Tele2 « *ne tranche pas la question de savoir si des traitements de données institués aux fins de la sauvegarde de la sécurité publique, la défense et la sûreté de l'Etat pour la mise en œuvre des activités des services de renseignement des Etats, relèvent de la clause d'exclusion prévue à l'article 1er, paragraphe 3, de la directive 2002/58* ».

En effet, au point 73 de son arrêt, **la Cour ne limite pas son raisonnement à la lutte contre la criminalité** (qu'elle ne mentionne explicitement que pour répondre aux questions d'espèce qui lui sont posées) mais couvre bien toutes les finalités (dont celles évoquées par le Premier ministre) visées par l'article 15 de la directive :

> « *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.* »

Ainsi, les mesures mises en œuvre pour la sauvegarde de la sécurité nationale n'échappent pas au champ d'application de l'article 15 de la directive 2002/58 et, par-là, de la Charte.

Puisque c'est au regard du principe de proportionnalité imposé par la Charte que les solutions de l'arrêt *Tele2* ont été retenues, ces mesures doivent aussi respecter ces solutions.

En définitive, les solutions retenues par l'arrêt Tele2 s'appliquent à l'ensemble des mesures de renseignement concernées par la présente affaire, soit car la grande majorité de ces mesures concernent la lutte contre la criminalité et sont donc déjà directement visées par cet arrêt, soit car une minorité de ces mesures, concernant la sécurité nationale, doivent respecter la Charte, en application de laquelle ces solutions ont été retenues.

Sur la disproportion du régime de conservation des données

III. En deuxième lieu, le Premier ministre tente de démontrer que la **proportionnalité** d'un régime de conservation généralisée serait évaluée différemment selon que ce régime poursuive des finalités de lutte contre la criminalité – ce qui est l'espèce de l'arrêt *Tele2* – ou « *des fins de sauvegarde de la sécurité publique, la défense et la sûreté de l'État* ».

Il prétend que ce dernier régime, limité à ces finalités, satisferait les exigences de proportionnalité imposées par la Charte.

III-1 À titre liminaire, il faut encore rappeler que la « *sécurité publique* » est, en droit de l'Union, déjà comprise par la finalité de « *lutte contre la criminalité* » et que la distinction qu'en fait le Premier ministre n'est donc pas valable.

De plus, il faut souligner que la proportionnalité du régime de conservation généralisée français doit être évaluée au regard de l'ensemble des finalités qu'il poursuit, et non pas d'une minorité d'entre elles – la sauvegarde de la sécurité nationale – qui, à elle seule, ne pourrait certainement pas rendre proportionnel l'ensemble de la mesure.

La démonstration que le Premier ministre tente ici de faire valoir est donc vaine.

III-2 C’est tout aussi vainement que le Premier ministre prétend que l’hypothétique régime de conservation généralisée qui s'inscrirait dans le seul cadre de la sécurité nationale serait proportionné.

III-2.1 S'agissant d’abord du caractère **nécessaire** d'un tel régime, l’argumentation du Premier ministre repose sur une simple affirmation – au demeurant étayée par strictement aucun document, ni aucune preuve – : « *L'expérience des services de renseignement montre que les renseignements ainsi obtenus peuvent apporter une contribution essentielle en matière de prévention du terrorisme, de contre-espionnage ou encore de lutte contre la prolifération* ».

Si cette affirmation pouvait être précisément démontrée, la CNCIS, la CNCTR ou la délégation parlementaire au renseignement auraient eu l'occasion de le faire dans au moins un de leurs nombreux et détaillés rapports.

Pourtant, de façon pour le moins éloquente, le Premier ministre ne justifie aucunement ses assertions à l’aune de ces dernières sources.

Au demeurant, comme les exposantes l’ont déjà démonté, l'arrêt ***Tele2*** **exclut déjà** que la prévention du **terrorisme** – explicitement mentionnée – soit une finalité susceptible de rendre proportionnel un régime de conservation généralisée.

C’est donc en vain que le Premier ministre s’en prévaut.

III-2.2 S’agissant ensuite du caractère adapté de la mesure de conservation ciblée, le Premier ministre prétend que cette mesure – présentée comme la seule mesure proportionnée selon l'arrêt *Tele2* – serait « *inadaptée aux finalités spécifiques de sauvegarde de la sécurité publique, la défense et la sûreté de l'État* ».

Pour tenter d'étayer une telle affirmation, le Premier ministre indique que la conservation ciblée – à la différence de la conservation généralisée – « *permettrait de* ***caractériser une menace*** *préalablement identifiée et, le cas échéant, d'y parer, mais serait inadapté[e] pour* ***identifier les menaces*** *elles-mêmes* ».

Une telle affirmation peut être admise mais révèle alors combien la démonstration du Premier ministre est erronée concernant la conservation généralisée, laquelle apparait ainsi comme systématiquement disproportionnée.

En effet, le Premier ministre explique ici que la conservation généralisée est un préalable nécessaire pour « *identifier* » ou « *découvrir* » des menaces jusqu'alors inconnues.

Or, de telles « *découvertes* » ne sont possibles qu'en surveillant activement – notamment en accédant au contenu de leurs communications – **des personnes sur qui ne pèse encore aucun soupçon** de présenter une menace.

Sans de telles surveillances, il ne s'agirait pas de « *découvrir* » mais simplement de « *caractériser* » ou de « *vérifier* » des menaces déjà suspectées.

Par définition, l'ensemble de la population entre dans cette catégorie de personnes.

Ces « *découvertes* » constituent donc des mesures de **surveillance généralisée**, susceptibles de concerner n'importe quelle personne, sans qu'aucun critère n'en limite le champ.

A ce titre, et au regard de la Charte, elles ne peuvent jamais passer pour proportionnées, car elles portent atteinte au contenu essentiel des droits au respect des communications et de la vie privée, tels que garantis par les articles 7 et 8 de la Charte.

Ainsi, de l'aveu du Premier ministre, la conservation généralisée n'est nécessaire qu'en tant que préalable à des mesures de surveillance généralisée, intrinsèquement disproportionnées.

Partant, la conservation généralisée ne peut elle-même qu'être disproportionnée.

III-3 Il est d'ailleurs pour le moins révélateur qu'au fil de ses développements, le Premier ministre en vient à abandonner ce raisonnement.

Il admet ainsi que, dans le cadre du régime actuel de conservation généralisée, « *en pratique, l'accès aux données conservées fait nécessairement l'objet d'un ciblage puisque les demandes d'accès doivent s'appuyer sur un motif précis tenant à l'existence d'informations obtenus* ***par un autre biais*** *ou par l'utilisation* ***d'une autre technique*** *de renseignement* ».

Les données conservées de façon généralisée ne sont donc **pas utilisées pour « *découvrir* » des menaces**, mais simplement pour confirmer ou « *caractériser* » des menaces préalablement identifiées par d'autres moyens.

C'est exactement ce que permet aussi de faire la conservation ciblée, telle que le Premier ministre la décrit dans son raisonnement cité ci-avant.

De l'aveu du Premier ministre, « *en pratique* », **la conservation généralisée et celle ciblée permettent de poursuivre les mêmes objectifs :** « *caractériser* » des menaces, et non en « *découvrir* ».

La conservation ciblée portant une atteinte plus faible aux droits et libertés garanties par la Charte, la conservation généralisée n'est ni nécessaire ni proportionnée.

Sur la transmission d'une question préjudicielle

IV. En troisième lieu, et à titre subsidiaire, le Premier ministre fait valoir que la Cour de justice devrait modifier en profondeur l'interprétation qu'elle fait de la Charte dans ses différents arrêts *Tele2*, *Schrems* (C-362/14) et *Digital Rights Ireland* (C-293/12).

Pour ce faire, il invite le Conseil d'État à soumettre ce débat à la Cour dans le cadre d'une **question préjudicielle**.

Puisque les requérantes ont-elles-mêmes déjà invité le Conseil d'Etat à poser une telle question, elles ne peuvent que persister de plus fort dans leurs précédentes écritures sans anticiper sur la teneur du débat qui pourrait se tenir devant la Cour de justice.

Sur l'élargissement du périmètre des données auxquelles les services de renseignement peuvent accéder

V. En quatrième et dernier lieu, dans ses ultimes observations en réplique, le **ministre de l'intérieur** tente de s'opposer à l'argumentation développée par les requérantes contre la légalité de **l'élargissement du périmètre des données auxquelles les services de renseignement peuvent accéder**, tel que réalisé par l'article 2, 3°, du décret n° 2016-67.

V-1 À titre liminaire, il faut de souligner que le ministre se méprend sur les termes du débat lorsqu'il expose, en introduction de la partie C de ses observations, puis au point 2 de cette même partie, que les requérantes feraient valoir que, par ce décret, « *le pouvoir réglementaire aurait imposé un même régime de conservation des données tant aux opérateurs de communications électroniques qu'aux fournisseurs d'accès et hébergeurs* ».

Puisque l'article 2, 3°, du décret attaqué n'altère pas le régime de conservation des données, mais seulement celui de leur recueil par les services de renseignement, il n'est manifestement pas inutile de rappeler que les requérantes n'ont jamais contesté ce dispositif en de tels termes.

D'ailleurs, dans leurs observations déposées le 24 novembre 2017, les exposants introduisent explicitement leur raisonnement par l'intitulé suivant : « *Sur l'extension du périmètre des données de connexion recueillies* ».

V-2 Sur le fond, le ministre de l'intérieur reprend l'essence des arguments développés par les requérantes et les confirme donc.

V-2.1 Premièrement, ainsi que les requérantes l'ont déjà exposé, le ministre admet que le décret autorise un « *accès direct* » (en applications des articles L851-2 et L851-3 du CSI) à une plus large variété de données qu'il n'en autorise par « *accès différé* » (en application de l'article L851-1).

V-2.2 Deuxièmement, tout comme les requérantes l'ont aussi exposé, le ministre admet que, contrairement à la lettre de son texte, le décret autorise un « *accès direct* » à des données qui **peuvent révéler le « *contenu des correspondances échangées ou des informations échangées* ».**

Ce faisant, le ministre admet implicitement mais nécessairement que le périmètre de ces données dépasse celui délimité par la loi, tel qu'interprété par le Conseil constitutionnel.

En effet, ce dernier considère 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 [... qui]* ***ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit*** » (Cons. constit., Déc. n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement, cons. 55).

V-2.3 Troisièmement, et enfin, le ministre ne contredit pas le fait que le décret viole la loi en prévoyant **deux périmètres distincts** de données auxquelles il peut être accédé, selon que cet accès soit « *direct* » ou « *différé* », alors que le code de la sécurité intérieure, en faisant systématiquement référence à l'unique périmètre défini à son article L851-1, suit la démarche explicite de n'en prévoir qu'**un seul**, commun à tous les types d'accès.

En dépit de tout ce qui précède, le ministre de l'intérieur conclut à la légalité du décret.

Sans rejeter l’ensemble de son développement, qui vient principalement au soutien de l'argumentation des requérantes, la conclusion du ministre ne peut ainsi qu'être écartée.

VI. En définitive, donc, l’ensemble des décrets attaqués sont voués à la censure, le cas échéant après renvoi d’une question préjudicielle à la Cour de justice de l’Union européenne.

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.

Avec toutes conséquences de droit.

SPINOSI & SUREAU
SCP d’Avocat au Conseil d’État