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

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

Sur la requête n° 388.134

DISCUSSION

I. En réponse au mémoire en défense en date du 6 octobre 2015 déposé par le Premier ministre, les associations French Data Network (FDN) et La Quadrature du Net ainsi que la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) entendent verser aux débats les observations suivantes.

Persistant dans l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures, les exposantes entendent plus particulièrement stigmatiser la lecture partielle et erronée faite par la partie défenderesse du droit applicable en l'espèce.

Sur l'absence de compétence du pouvoir réglementaire

II. En premier lieu, le Premier ministre tente de faire valoir que le pouvoir réglementaire était bien compétent pour édicter le décret attaqué (cf. le mémoire en défense, p. 2).

Mais le raisonnement développé par le Premier ministre lui-même confirme qu'il n'en est strictement rien.

II-1 En effet, pour justifier de la nécessité de définir par le décret visé à l'article L. 246-4 du code de la sécurité intérieure les données pouvant être recueillies ainsi que les services de l'Etat bénéficiaires, le Premier ministre soutient tout d'abord que, dès lors qu'il lui appartenait de préciser les conditions de fonctionnement de la Commission nationale de contrôle des interception de sécurité (CNCIS), il lui fallait également définir les données auxquels pourraient avoir accès des services, lesquels devant aussi être déterminés.

Un tel raisonnement revient, implicitement mais nécessairement, à considérer que lorsqu'une procédure de contrôle doit être définie par décret, il doit *ipso facto* en être déduit qu'il revient aussi au pouvoir réglementaire de déterminer les atteintes aux libertés fondamentales sur laquelle la procédure de contrôle est censée porter.

Or, il convient de rappeler qu'aux termes de l'article 34 de la Constitution, c'est à « *la loi* » qu'il revient de fixer « *les règles concernant […] les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » (sur l'exigence européenne d'encadrement légal, v. également CJUE, Grande Chambre, 8 avril 2014, Aff. C-293/12 et C-594/12).

II-2 En outre, l'argumentation développée par le Premier ministre, en particulier pour préciser la mission de la CNCIS, témoigne de ce que le pouvoir règlementaire a manqué à son office en ne désignant ni les données, ni les services concernés.

Plus encore, les dispositions règlementaires litigieuses n'ont pas davantage défini les procédures de suivi des demandes et de conservation des documents transmis à l'administration (cf. le point 4.2. de la requête introductive), ce que ne conteste aucunement le Premier ministre.

Pourtant, ainsi que l'a récemment rappelé le Conseil constitutionnel, c'est à la loi qu'il appartient de déterminer « *les conditions d'exploitation, de conservation et de destruction des renseignements collectés* » (Cons. constit. Déc. n° 2015-713 DC du 23 juillet 2015, cons. 78).

Il résulte ainsi de ce qui précède que, contrairement à ce que soutient le Premier ministre, le pouvoir réglementaire a clairement excédé sa compétence en édictant les dispositions du décret attaqué.

Sur l'absence de notification du projet de décret à la Commission européenne

III. En deuxième lieu, dans l'espoir de justifier la méconnaissance de l'obligation de notification du projet de décret contestée à la Commission européenne en vertu de l'article 10 de la directive 98/34/CE du 22 juin 1998, le Premier ministre tente de faire valoir que le décret litigieux n'entrerait pas dans le champ d'application de cette directive (cf. le mémoire en défense, p. 3).

Or, une telle tentative ne peut qu'être vaine.

III-1 D'une part, et de manière pour le moins aventureuse, le Premier ministre prétend que « *les obligations fixées par la directive [...] ne peuvent s'appliquer à des normes décidées par les Etats membres pour des motifs de sécurité nationale* » en arguant de ce que l'article 4 du traité sur l'Union européenne stipule que « *la sécurité nationale reste de la seule responsabilité de l'Etat membre* » (cf. le mémoire en défense du Premier ministre, page 3).

Or, **d'emblée**, il importe de relever qu'admettre un tel raisonnement reviendrait à tolérer qu'un Etat membre de l'Union puisse se soustraire à ses obligations issues du droit de l'Union européenne au seul motif qu'il a spontanément décidé de placer l'un de ses dispositifs sous le sceau de la sécurité nationale.

Surtout, une telle lecture du Premier ministre ne résiste pas à l'analyse des textes pertinents et de la jurisprudence européenne.

Ainsi, l'obligation de communication de tout projet de règle technique prévue par l'article 8 de la directive 98/34/CE du 22 juin 1998 n'est écartée que dans les situations limitativement énumérées au sein de l'article 10 du même texte et l'enjeu de la sécurité nationale n'y figure absolument pas.

En outre, le champ d'application de la directive 98/34/CE du 22 juin 1998 n'est lui-même aucunement restreint par les impératifs tenant à la sécurité nationale.

Plus généralement encore, il y a lieu de rappeler que le droit de l'Union européenne peut parfaitement régir des domaines affectant la sécurité nationale sans que le principe prévu à l'article 4.2 du traité sur l'Union européenne ne soit méconnu.

Pour s'en convaincre, et parmi de multiples autres exemples, il suffit de rappeler le récent arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire *Digital Rights Ireland et Seitlinger e.a* (CJUE, Grande Chambre, 8 avril 2014, Aff. C-293/12 et C-594/12).

A cette occasion, la Cour de justice était appelée à apprécier de la validité de la directive 2006/24/CE du 15 mars 2006 sur la

conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, laquelle fut notamment adoptée pour agir face « *aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme* » et prévenir de nouveaux attentats terroristes à l'instar de ceux de Londres en 2005 (considérants 9 et 10 de la directive).

Ainsi, il est manifeste que le droit dérivé de l'Union européenne est intervenu dans le domaine de la sécurité nationale sans méconnaître le champ de compétence de l'Union. Au demeurant, si la Cour de justice n'a pas hésité à invalider ce texte, c'est uniquement en raison de la méconnaissance par cette directive des exigences du droit originaire de l'Union, au premier rang desquels figure la Charte des droits fondamentaux de l'Union européenne (v. *Digital Rights Ireland et Seitlinger e.a*, précité, § 32-71).

Enfin, à supposer même qu'il soit possible – pour les seuls besoins de la discussion – d'admettre un seul instant la lecture du Premier ministre selon lequel les obligations de la directive 98/34/CE ne s'appliqueraient pas aux dispositifs nationaux relatifs à la sécurité nationale, il convient de relever le dispositif d'accès administratif aux données de connexion mis en œuvre par le décret contestées ne concerne pas ce seul impératif.

En effet, aux termes des dispositions de l'article L. 241-2 du code de la sécurité intérieure en vigueur au jour de l'introduction du présent recours en annulation, les techniques d'accès administratif aux données de connexion pouvaient être mise en œuvre pour « *rechercher des renseignements intéressant la sécurité nationale* » mais aussi « *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1* » du même code.

III-2 D'autre part, le Premier ministre ne saurait pas davantage écarter l'applicabilité de la directive du 22 juin 1998 en affirmant que « *le décret ne constitue pas une règle technique ni une règle technique*

ni une règle relative aux services au sens de l'article 1er de la directive » (Mémoire en défense, page 3).

En effet, à rebours de ce qu'affirme le Premier ministre, le décret litigieux affecte bien les conditions dans lesquelles les opérateurs peuvent s'installer ou exercer leur activité sur le territoire national, dès lors qu'il définit les conditions dans lesquelles les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs doivent déférer à un ensemble d'obligations destinées à offrir aux services compétents un accès aux données de connexion au sens des articles L. 246-1 et suivants du code de la sécurité intérieure.

Cette seule circonstance suffit à caractériser une « *règle technique* » au sens de l'article 1er 11) de la directive 98/34/CE modifiée, en ce que ces dispositions précisent qu'une telle règle est « *une spécification technique ou autre exigence ou une règle relative aux services, y compris les dispositions administratives qui s'y appliquent, dont l'observation est obligatoire de jure ou de facto, pour la commercialisation, la prestation de services, l'établissement d'un opérateur de services ou l'utilisation dans un État membre ou dans une partie importante de cet État […]* ».

Puisqu'en vertu de l'article 1er de la directive 98/48/CE portant modification de l'article 1er de la directive 98/34/CE, les services ainsi visés renvoient à « *tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* », il ne fait guère de doute que sont concernés l'ensemble des prestations offertes par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs.

IV. Partant, la seule absence de notification du décret litigieux à la Commission européenne caractérise un vice de procédure qui en justifie la censure (v. not. CE, 10 juin 2013, n° 327.375).

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

V. En troisième lieu, le Premier ministre n'hésite pas à soutenir que le moyen tiré de la violation de Charte des droits fondamentaux serait

inopérant dès lors que le décret attaqué ne mettrait pas en œuvre le droit de l'Union européenne (cf. le mémoire en défense, p. 4).

Là encore, une telle affirmation pourra être aisément écartée.

V-1 En effet, et en droit, la seule circonstance que les mesures litigieuses relèvent de la sécurité nationale ne saurait avoir pour conséquence de les soustraire du droit de l'Union européenne, dès lors que ces mesures constituent une limitation des droits et obligations résultant de la mise en œuvre du droit de l'Union.

Or, il appartient bien au Conseil d'État d'examiner si le décret attaqué constitue effectivement une telle mesure de limitation de la mise en œuvre du droit de l'Union.

Toute autre interprétation reviendrait à priver l'article 51-1 de la Charte des droits fondamentaux de tout effet utile, puisqu'il suffirait à chaque Etat membre de revendiquer la poursuite d'un objectif de sécurité nationale pour soustraire n'importe quelle mesure du contrôle de conventionnalité.

V-2 En outre, et toujours en droit, le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques font incontestablement partie du champ matériel du droit de l'Union européenne, qu'il s'agisse des articles 7 et 8 de la Charte ou de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

V-2.1 En particulier, l'objet de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 (directive dite « ePrivacy ») vise « *à garantir le plein respect des droits exposés aux articles 7 et 8* » de la Charte des droits fondamentaux (considérant 2).

Cette volonté du législateur européen apparaît notamment à l'article 15 de la directive, lequel établit les conditions dans lesquelles les États membres peuvent, dans la mise en œuvre du droit de l'Union,

prendre des mesures législatives ayant pour objectif notamment la sauvegarde de la sécurité nationale :

« *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.* »

L'application de cet article à des mesures pour la sauvegarde de la sécurité nationale appelle deux remarques.

Tout d'abord, et contrairement à ce que soutient le Premier Ministre, le fait que les mesures litigieuses soient motivées par la sauvegarde de la sécurité nationale ne saurait avoir pour conséquence de les soustraire au respect du droit de l'Union européenne.

En effet, les mesures poursuivant un objectif de sauvegarde de la sécurité nationale sont explicitement visées par l'article 15 précité.

Ensuite, l'article 15 de la directive 2002/58 prévoit que de telles mesures visant à sauvegarder la sécurité nationale comprennent « *entre autres* » des mesures législatives prévoyant la conservation de données. La directive n'exclut donc pas de son champ d'application les mesures prévoyant l'accès aux données conservées ainsi que les modalités du contrôle de cet accès aux données conservées et leur utilisation subséquente.

Au contraire, de telles mesures s'inscrivent dans un ensemble

juridique cohérant relatif à la conservation des données dans l'objectif de sauvegarder la sécurité nationale.

Partant, toute mesure nationale ayant pour objectif la sauvegarde de la sécurité nationale doit être adoptée dans le respect de la Charte des droits fondamentaux de l'Union européenne, dès lors qu'une telle mesure constitue une limitation des droits et des obligations qui sont une mise en œuvre du droit de l'Union.

V-2.2 Plus particulièrement encore, l'article 15 de la directive précitée mentionne explicitement les droits et obligations en matière de confidentialité des communications et d'anonymisation des données définis par les articles 5, 6, 8, paragraphes 1, 2, 3 et 4, et par l'article 9 de la directive 2002/58.

Ces dispositions créent à la charge des États membres une obligation de garantir le respect de la vie privée ou du secret des correspondances en matière de communications électroniques et des données personnelles afférentes.

L'article 5, intitulé « Confidentialité des communications », prévoit ainsi que :

« *1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. [...]* »

L'article 6 portant sur les « Données relatives au trafic » précise pour sa part que :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1. [...] »

Enfin, aux termes de l'article 9 relatif aux « Données de localisation autres que les données relatives au trafic »

« *1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic. [...] »*

VI. Or, **en l'espèce**, il ne fait aucun doute que les mesures litigieuses, lesquelles devraient être nécessaires, appropriées et proportionnées dans une société démocratique, constituent bien une limitation des droits et obligations précités.

En effet, l'article L. 246-1 (entretemps modifié et prévu désormais à l' article L. 851-1) du code de la sécurité intérieure porte notamment sur le recueil par l'administration, auprès des opérateurs de communications électroniques et des hébergeurs, des « *données techniques [...] de connexion à des services de communications électroniques* », des données relatives « *à la localisation des équipements terminaux utilisés* » et, plus généralement le recueil des

données conservées en application de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ainsi que du II de l'article 6 de la loi n° 2004-575 dite LCEN (v. Cons. const., juillet 2015, décision QPC n° 2015-478, cons. 12).

Or, les données ainsi visées par les dispositions litigieuses recouvrent totalement les données visées par les articles 5, 6, 8, paragraphes 1, 2, 3 et 4, et par l'article 9 de la directive 2002/58 précités, à savoir notamment les données relatives au trafic et les données de localisation.

Il ne saurait donc être sérieusement contesté que les dispositions litigieuses, en permettant à l'administration le recueil des données visées, constituent une limitation aux principes de confidentialité, d'effacement et d'anonymisation de ces données tels que prévus par le droit de l'Union.

VII. Ainsi, et contrairement à ce que tente vainement de démontrer le Premier Ministre, dès lors qu'elles constituent bien une limitation aux droits ou obligations résultant de la mise en œuvre du droit de l'Union, les mesures litigieuses doivent respecter la Charte des droits fondamentaux de l'Union européenne.

Toute autre appréciation révèlerait nécessairement l'existence d'une difficulté réelle et sérieuse d'interprétation des stipulations des traités de l'Union européenne – parmi lesquels figure la Charte des droits fondamentaux – mais aussi des dispositions des actes de droit dérivé – dont en particulier les directives 95/46/CE du 24 octobre 1995 et 2002/58/CE du 12 juillet 2002.

Or, **une telle situation exigerait nécessairement qu'une question préjudicielle soit adressée à la Cour de justice de l'Union européenne** en application de l'article 267 du Traité sur l'Union européenne, et plus précisément encore de son alinéa 5 qui prévoit une obligation de renvoi préjudiciel pour les juridictions nationales qui, à l'instar du Conseil d'Etat, rendent des « *décisions [qui] ne sont pas susceptibles d'un recours juridictionnel de droit interne* ».

Sur la méconnaissance de la Charte des droits fondamentaux de l'Union européenne

VIII. En quatrième lieu, le Premier ministre avance que le dispositif d'accès administratif aux données de la connexion n'est pas contraire aux stipulations de la Charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014 (cf. le mémoire en défense, p. 4).

Une fois encore, l'argumentation du Premier ministre ne saurait convaincre.

VIII-1 En effet, il importe à nouveau de souligner que la directive 2006/24/CE a été invalidée par la Cour de justice en ce qu'elle ne prévoyait « *pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 65) et manquait ainsi « *de garantir qu'elle [était] effectivement limitée au strict nécessaire* ».

Cette exigence de nécessité à laquelle doit se conformer toute ingérence dans les droits fondamentaux est fondée aussi bien sur l'article 52, paragraphe 1 de la Charte des droits fondamentaux que sur une jurisprudence constante de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne.

Venant préciser les critères de stricte nécessité qu'elle avait alors dégagés dans l'arrêt *Digital Rights,* la Cour de justice de l'Union européenne a clairement établi, dans son arrêt *Schrems* du 6 octobre 2015 (point 93), que « *n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes* » sans,

- D'une part, « *qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi* » (section 1.2.1) ;

- D'autre part, sans « *que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur*

utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence » (section 1.2.2) (CJUE, 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner,* Aff. C-362/14).

Or, le régime français en matière de conservation généralisée des données et d'accès à ces données présente précisément ces deux défauts.

Plus particulièrement, le décret attaqué en matière d'accès administratif aux données de connexion ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence d'accéder à ces données conservées.

VIII-2 Par ailleurs, en rappelant la nécessité de limiter le champ des données conservées, le récent arrêt *Schrems* s'inscrit dans une ligne jurisprudentielle déjà définie par la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne.

Ainsi, par stricte application de l'article 8 de la Convention européenne des droits de l'homme, la Cour de Strasbourg encadre le champ des données à caractère personnel pouvant être collectées et conservées à des fins d'intérêt général en considérant que :

« *La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article [...] La nécessité de disposer de telles garanties se fait d'au- tant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières.* ***Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées*** » (Cour EDH*,* Grande Chambre, 4 décembre 2008, *Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, §103*)*

Lors de l'examen de la directive 2006/24/CE, la Cour de justice de l'Union européenne a dénoncé avec une particulière insistance la gravité de l'ingérence dans la vie privée des personnes que constitue la simple conservation de leurs données de connexion :

« *Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. [...]*

Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme ***particulièrement grave.*** *En outre, la circonstance que la conservation des données* ***et l'utilisation ultérieure de celles-ci*** *sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.* » *Digital Rights Ireland et Seitlinger e.a*, précité, § 27 et 37).

A fortiori, les données conservées auxquelles l'administration a la faculté d'accéder révèlent donc des informations particulièrement personnelles, une telle faculté constituant par conséquent une grave ingérence.

VIII-3 En outre, la Cour de justice de l'Union européenne conditionne la validité des régimes d'accès aux données issues d'une obligation de conservation généralisée à la présence de critères objectifs limitant l'accès et l'utilisation subséquente à des finalités poursuivies suffisamment sérieuses, c'est-à-dire des finalités « *précises, strictement restreintes et susceptibles de justifier l'ingérence* ».

Dans son arrêt *Digital Rights* précité, elle constatait ainsi que :

« *La directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence.* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 60)

En 2015, la Cour de justice a repris et précisé ce critère dans son arrêt *Schrems* en l'érigeant en critère de validité de tout régime d'utilisation des données relatives au trafic.

Ainsi, emporterait nécessairement violation de la Charte un régime qui ne prévoirait pas « *un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* » (*Maximillian Schrems contre Data Protection Commissioner,* précité, § 93).

IX. Or**, en l'espèce** et **premièrement**, il est manifeste que le décret attaqué ne prévoit aucun critère objectif permettant de limiter l'accès aux données de connexion.

Dans sa version en vigueur au jour de l'introduction du présent recours, l'article L. 246-1 du code de la sécurité intérieure disposait que :

« *Pour les finalités énumérées à l'article L. 241-2, 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. »

Ces dispositions ont depuis été transférées, après modification, à l'article L. 851-1 du code de la sécurité intérieure.

Or, à aucun moment les dispositions réglementaires attaquées ou les dispositions législatives sur lesquelles elles se fondent n'établissent de critères objectifs venant limiter ou à tout le moins définir l'accès des services administratifs aux données que tant les hébergeurs que les fournisseurs de services de communications électroniques doivent conserver.

X. Par ailleurs, et **deuxièmement**, le décret attaqué renvoie à des finalités imprécises et peu restreintes.

La disposition contestée renvoie en effet aux finalités de l'article L. 241-2 de code de la sécurité intérieure, à savoir :

« rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1. »

Or, de tels objectifs sont si largement définis et d'une telle diversité qu'ils ne peuvent en aucun cas être considérés comme « *des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* ».

En effet, il peut être difficilement soutenu que « *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* » constitue une finalité précise, dès lors que les « *éléments essentiels* » visés ne sont définis par aucune disposition légale ou règlementaire. Au contraire, elles sont unilatéralement déterminées par les seules autorités administratives lorsqu'elles recourent à des

mesures de surveillance, sans même que les critères définissant ces « *éléments essentiels* » ne soient connus du public.

Dans ces conditions, il ne saurait être sérieusement soutenu qu'une telle finalité soit strictement restreinte.

De plus, la « *criminalité et la délinquance organisées* » recouvrent les nombreuses infractions listées à l'article 706-73 du code de procédure pénale (voir Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015).

Au titre de celles-ci se trouvent par exemple les infraction définies aux articles 222-34 à 222-40 du code pénal dont, notamment, la détention, l'acquisition ou l'emploi illicites de stupéfiants à titre personnel.

Or, la prévention de telles infractions ne serait nullement susceptible de justifier l'ingérence permise.

XI. En outre, et **troisièmement,** les dispositions règlementaires attaquées définissent un champ particulièrement large des personnes ayant accès aux données de connexions.

Alors que la liste des services pouvant accéder aux données conservées par les opérateurs et hébergeurs était déjà particulièrement large, celle-ci a en effet encore été considérablement allongée par le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

Cette extension n'a néanmoins pas été associée à une partition des services administratifs selon les données auxquelles ils pouvaient avoir accès et les finalités pour lesquelles ils pouvaient y avoir accès.

Au contraire aux finalités déjà énoncées, dont la particulière imprécision a déjà été amplement soulignée, sont venues s'ajouter celles énoncées à l'article L. 811-3 du code de la sécurité intérieure.

Pourtant, la Cour de justice de l'Union européenne a considéré que la

limitation au strict nécessaire n'était pas garantie par la directive en ce qu'elle ne prévoyait « *aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 60).

L'importance de la définition précise et limitée du nombre d'administrations pouvant avoir accès aux données recueillies a encore récemment été mise en exergue par l'arrêt de la High Court britannique annulant la loi nationale adoptée l'an passé (High Court of Justice, 17 juillet 2015, [2015] EWHC 2092).

En effet, selon la Cour britannique, la loi nationale ne circonscrivait pas suffisamment le champ des autorités administratives pouvant accéder aux données que les opérateurs étaient tenus de conserver.

C'est d'ailleurs sur cette seule exigence que la *High Court* du Royaume-Uni a annulé une loi nationale établissant une obligation de conservation de données sans circonscrire suffisamment le champ des autorités administratives pouvant y accéder, considérant ainsi, dans un arrêt *Open Rights Group and others v. Secretary of State for the Home Department,* rendu le 17 juillet 2015, que :

« *La solution à ce problème et l'idée sous-jacente à l'arrêt Digital Rights Ireland est, selon nous, qu'une loi établissant un régime général de conservation de données de connexion viole les droits reconnus aux articles 7 et 8 de la Charte de l'UE à moins d'être accompagné par un régime d'accès (établi au niveau national) offrant des garanties adéquates de ces droits* » (§ 89 – Trad. libre de : « *The solution to the conundrum, in our view, and the ratio of Digital Rights Ireland, is that legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter unless it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights* »)

XII. Enfin, et **en quatrième et dernier lieu,** le décret attaqué n'a mis en place aucun contrôle préalable effectif.

Pourtant, dans son arrêt *Digital Rights*, la Cour de justice a clairement

énoncé que :

« *Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi*. » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 62)

Or, en l'espèce, les dispositions contestées ne prévoient que l'intervention d'une personnalité qualifiée placée auprès du Premier ministre en guise de contrôle préalable (article L. 246-2 du code de la sécurité intérieure).

Le seul contrôle préalable est donc celui d'une autorité qui n'est ni une autorité administrative indépendante, ni une juridiction et dont les critères d'appréciation ne sont pas clairement définis.

L'encadrement du rôle de la personnalité qualifiée et son positionnement auprès du Premier ministre ne permettent ainsi en aucune mesure de « *limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire* » (point précité).

XIII. Il résulte ainsi de l'ensemble de ce qui précède qu'à l'inverse de ce qu'affirme le Premier ministre, le décret attaqué méconnait clairement les stipulations de la Charte des droits fondamentaux de l'Union européenne, telle qu'interprété par la Cour de Justice dans son arrêt du 8 avril 2014.

Là encore, toute autre issue révèlerait une difficulté réelle et sérieuse d'interprétation des stipulations des traités de l'Union européenne et des dispositions des actes de droit dérivé, ce qui justifierait impérativement le renvoi par le Conseil d'Etat d'une **question préjudicielle** en application de l'article 267 du Traité sur l'Union européenne.

Sur la méconnaissance des dispositions de l'article L. 246-4 du code de la sécurité intérieure

XIV. En cinquième lieu, le Premier ministre tente de faire valoir que l'accès permanent de la CNCIS « *aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7* » suffirait à répondre à l'obligation de définir « *la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis* » que le Premier ministre déduit des dispositions de l'article L. 246-4 du code de la sécurité intérieure alors en vigueur.

XIV-1 Pourtant, une simple comparaison des articles L. 246-4 et R. 246-8 du code de la sécurité intérieure suffit à montrer l'absence de tout rapport entre les deux dispositions.

La première concerne en effet le suivi des demandes et les conditions de conservation des informations et documents transmis, quand la seconde porte sur l'accès à ces informations et documents par la CNCIS.

Dans ces conditions, le seul accès de la CNCIS ne saurait pallier les insuffisances flagrantes d'encadrement de « *la procédure de suivi des demandes et des conditions et durée de conservation des informations ou documents transmis* ».

XIV-2 A cet égard, il y a lieu de rappeler que la Cour de justice de l'Union européenne a érigé les modalités de conservation des données par les services en l'une des conditions de validité d'un système de conservation des données avec la Charte des droits fondamentaux de l'Union européenne.

Ainsi, dans son arrêt *Digital Rights*, la Cour de justice a jugé à propos des données conservées par les opérateurs que :

« *De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive*

2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles. » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 66).

A fortiori, une telle conclusion s'impose également aux administrations qui traitent ces données.

XIV-3 Or, en l'espèce, il est manifeste que rien n'est prévu dans le décret attaqué ou dans une quelconque autre disposition pour assurer la sécurité des données conservées une fois celles-ci transmises à l'administration.

XV. A tous égards, donc, la censure du décret attaqué est certaine.

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

Avec toutes conséquences de droit.

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