

Hugo ROY | Avocat à la Cour
1 rue Paul Baudry, 75008 Paris
Barreau de Paris, P.445

Conseil d'État
Section du contentieux
Formation spécialisée
N° 404013

Mémoire en réplique

POUR

Sophia Helena in 't Veld
[censuré]

CONTRE

Le Premier ministre
Hôtel Matignon, 57 rue de Varenne, Paris.

Au titre de l'article L. 773-1 du code de justice administrative

Recours formé en application du 1° de l'article L. 841-1 du code de la sécurité intérieure par lequel la requérante entend vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard.

TABLE DES MATIÈRES

Discussion	1
1 Sur la recevabilité et l'articulation des articles L. 841-1 et L. 854-9 CSI	2
2 Sur la recevabilité au regard de la directive 2016/680	4
3 Sur le fond	5
3.1 Sur la mise en œuvre du droit de l'Union	6
3.2 Sur l'atteinte au contenu essentiel du droit au respect de la vie privée	8
3.3 Sur le défaut de limitation au strict nécessaire	11
3.4 Sur l'absence d'information de la mesure de surveillance	17
3.5 Sur l'absence de procès équitable et de protection juridictionnelle effective	21
3.6 Questions préjudicielles	27
Table des jurisprudences	29

DISCUSSION

- 1 Dans l'instance n° 404013, le Premier ministre a déposé, le 26 janvier 2017, un mémoire en défense. Ce mémoire appelle les observations qui suivent, mais il ne modifie en rien l'argumentation précédemment développée dont la requérante entend conserver l'entier bénéfice.
- 2 En premier lieu, concernant la recevabilité de la requête et l'objet du litige, Madame In 't Veld entend, par le présent recours, faire procéder aux vérifications de mesures de surveillance internationale prises depuis 2008, notamment celles révélées par *L'Obs*¹. Le Premier ministre soutient qu'elle ne peut utilement se prévaloir de l'illégalité de telles mesures et que la présente demande de vérification serait fondée sur le mauvais article du code de la sécurité intérieure. Le Premier ministre se prévaut pour cela d'une décision de la formation spécialisée (Conseil d'État, form. spé., 19 oct. 2016, *A... D...*, n° 396958). Or, contrairement à l'interprétation donnée par le Premier ministre, cet arrêt conforte le droit de la requérante d'obtenir la vérification des mesures de surveillance en cause (**section 1**).
- 3 En second lieu, concernant le fond du litige, tout en évitant de se prononcer sur le droit de l'Union européenne, le Premier ministre considère que le droit français applicable en l'espèce est conforme à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (la Convention).
- 4 Or, comme démontré *infra*, tant la procédure d'autorisation que celle de mise en œuvre des mesures de surveillance internationale au cause, qu'elles précèdent ou succèdent à l'entrée en vigueur des lois n° 2015-912 (ci-après, « Loi Renseignement ») et n° 2015-1556 (dite « Loi sur la Surveillance Internationale »), ne respectent ni l'article 8 de la Convention, ni les articles 7, 8, 11 et 52(1) de la Charte des droits fondamentaux de l'Union européenne (la Charte). Il en va de même des garanties nécessaires à l'exercice du droit à un recours effectif au titre de l'article 13 de la Convention et à la protection juridictionnelle effective garantie au titre de l'article 47 de la Charte. Il convient d'insister, enfin, sur le fait que le droit de l'Union européenne est bien applicable en l'espèce, ce qui justifie pleinement que les questions préjudicielles énoncées *infra* soient transmises à la Cour de justice de l'Union européenne (**section 3 page 5**).

1. Voir la section 1 page 1 du mémoire ampliatif du 13 novembre 2016

1. Sur la recevabilité et l'articulation des articles L. 841-1 et L. 854-9 CSI

- 5 Le Premier ministre prétend que la présente demande visant à ce qu'une vérification soit effectuée sur les mesures de surveillance internationale réalisées avant l'entrée en vigueur de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (ci-après, la « Loi sur la Surveillance Internationale ») serait irrecevable en ce que la solution dégagée par le Conseil d'État dans sa décision *M. A... D...* précitée est « pleinement transposable aux vérifications des mesures de surveillance internationale. »
- 6 Néanmoins, il revient à votre formation de reconnaître la demande de vérification des mesures de surveillance internationale antérieures à l'entrée en vigueur de la Loi sur la Surveillance Internationale comme recevable en ce qu'elle se fonde sur l'article L. 773-1 du code de justice administrative. Cet article permet en effet la saisine du Conseil d'État par toute personne mentionnée au 1° de l'article L. 841-1 du code de la sécurité intérieure (CSI) y compris contre des mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de l'article L. 854-9 CSI.
- 7 **En droit**, l'article L. 841-1 CSI dispose que :
- « Sous réserve des dispositions particulières prévues à l'article L. 854-9 du présent code, le Conseil d'État est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en oeuvre des techniques de renseignement mentionnées au titre V du présent livre.
- « Il peut être saisi par :
- « 1° Toute personne souhaitant vérifier qu'**aucune technique de renseignement** n'est irrégulièrement mise en oeuvre à son égard et justifiant de la mise en oeuvre préalable de la procédure prévue à l'article L. 833-4 ; [...] »
- 8 L'article L. 854-9 prévoit en son alinéa 5 que seuls le président ou au moins trois membres de la CNCTR peuvent saisir le Conseil d'État, en cas de constatation d'un manquement au chapitre IV du titre V du livre VIII CSI (régime créé par la Loi Surveillance Internationale, entrée en vigueur le 2 décembre 2015).
- 9 Dans sa décision *M. A... D...* du 19 octobre 2016 publiée au recueil Lebon, la formation spécialisée du Conseil d'État a décidé que :
- « [L]es dispositions [de l'article L. 841-1] s'appliquent aux techniques de renseignement **mises en oeuvre** à compter de la date de leur entrée en vigueur, soit le 3 octobre 2015, y compris celles qui, initiées avant cette date, **ont continué à être mises en oeuvre après.** »

- 10 La solution retenue par la formation spécialisée du Conseil d'État et pleinement applicable aux dispositions de l'article L. 854-9 (créé par la Loi sur la Surveillance Internationale). Dès lors, les dispositions de l'article L. 854-9 s'appliquent aux mesures de surveillance internationale mises en œuvre à compter de la date de leur entrée en vigueur, soit le 2 décembre 2015. *A contrario*, cela signifie que les dispositions de l'article L. 854-9 **ne sont pas applicables** (i) aux mesures de surveillance internationale mises en œuvre sur une période antérieure à la date d'entrée en vigueur de la Loi sur la Surveillance Internationale, ni (ii) aux mesures de surveillance qui, initiées avant cette date, **n'ont pas continué à être mises en œuvre après**.
- 11 Le Premier ministre le reconnaît d'ailleurs explicitement lorsqu'il écrit (en page 2 de son mémoire en défense) que « *la solution retenue par le Conseil d'État s'agissant des vérifications prévues à l'article L. 841-1 du CSI [...] est pleinement transposable aux vérifications des mesures de surveillance internationale* ». C'est par une lecture erronée de la décision *M. A... D...* précitée que le Premier ministre conclut que la demande de vérification portant sur la période antérieure à l'entrée en vigueur de la Loi sur la Surveillance Internationale ne pourrait qu'être rejetée.
- 12 En effet, l'exception à la règle de l'article L. 841-1 CSI ouverte en faveur de l'article L. 854-9 CSI est **sans effet** sur l'applicabilité des dispositions de l'article L. 841-1 CSI aux mesures de surveillance internationale **mises en œuvre** à compter du 3 octobre 2015, y compris celles qui, initiées avant cette date, ont continué à être mises en œuvre après et qui ont cessé à être mises en œuvre avant l'entrée en vigueur de la loi sur la Surveillance Internationale.
- 13 Dit autrement, l'article L. 841-1 CSI permet le contrôle par le Conseil d'État de l'ensemble des mesures de surveillance internationale dont la mise en œuvre a commencé **ou** a perduré après le 3 octobre 2015 **et** a cessé avant le 2 décembre 2015.
- 14 Cela est d'ailleurs conforme aux écritures du Premier ministre lorsque celui-ci souligne en page 3 de son mémoire en défense que « *le dispositif mis en place par la loi n° 2015-912 du 24 juillet 2015 [créant l'article L. 841-1 CSI dans sa version en vigueur du 3 octobre au 2 décembre] permet à toute personne [...] de saisir une juridiction [...] pour procéder à des vérifications* » et prévoit donc « *un recours **largement ouvert*** ».
- 15 Il ne fait donc aucun doute, de l'aveu du Premier ministre lui-même, que les dispositions résultant de la Loi Renseignement et précédant l'entrée en vigueur de la Loi sur la Surveillance Internationale, prévoient un recours ouvert à toute personne de saisir la formation spécialisée du Conseil d'État afin de procéder à des vérifications concernant les mesures de surveillance, y compris internationale.
- 16 **En l'espèce**, les mesures de surveillance internationale sur lesquelles porte la présente demande de vérification ont été mises en œuvre depuis 2008 et révélées par *L'Obs* en juillet 2015. Leur mise en œuvre a donc bien été initiée avant le 2 décembre 2015.

- 17 Qui plus est, ces mesures relèvent indubitablement de la mise en œuvre de techniques de renseignement mentionnées au titre V du présent livre VIII du code de la sécurité intérieure, que ce soit par leur caractère international mentionné expressément au chapitre IV, ou au titre des techniques de renseignement relevant des chapitres I à IV titre V du livre VIII (notamment l'accès ou le recueil de données de connexion).
- 18 Pour savoir si les dispositions de l'article L. 854-9 sont applicables à de telles mesures, encore faut-il déterminer si ces mesures ont continué à être mises en œuvre après le 2 décembre 2015, date d'entrée en vigueur de cet article.
- 19 Or, le Premier ministre n'apporte *aucun élément* tendant à démontrer que **toutes** les mesures de renseignement visées, mises en œuvre depuis 2008, auraient continué après la date d'entrée en vigueur de l'article L. 854-9 résultant de la Loi sur la Surveillance Internationale, soit le 2 décembre 2015. Pourtant, c'est bien sur lui que la charge de la preuve repose, les mesures en cause étant par définition secrètes. Il n'y a donc aucune raison que l'article L. 854-9 s'y applique.
- 20 **Par conséquent**, la formation spécialisée du Conseil d'État peut être saisie pour toute vérification des mesures de surveillance — y compris internationale — dont la mise en œuvre aurait cessé entre le 3 octobre et le 2 décembre 2015.
- 21 Pour cette raison, en l'absence d'éléments apportés par le Premier ministre tendant à démontrer que la totalité des mesures de surveillance internationale en cause aurait continué au-delà du 2 décembre 2015, la procédure de vérification ouverte par l'article L. 841-1 CSI est pleinement applicable aux mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de la Loi sur la Surveillance Internationale et s'impose en l'espèce.

2. Sur la recevabilité au regard de la directive 2016/680

- 22 Au surplus, le Conseil d'État devra interpréter les dispositions nationales en vigueur à la lumière de la directive 2016/680.
- 23 **En droit**, la Directive (UE) 2016/680 du 27 avril 2016 a pour objet et objectifs d'établir « 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 », et s'applique donc aux mesures de surveillance internationales en cause.
- 24 La Directive impose notamment que « sans préjudice de tout autre recours administratif ou extrajudiciaire, les États membres prévoient qu'une per-

- sonne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne » (Directive (UE) 2016/680, Article 53).
- 25 Or, suivant le principe de l'interprétation conforme, le juge national est tenu d'interpréter le droit en vigueur à la lumière de la directive destinée à faire l'objet d'une transposition (CJCE, 6^e, 8 oct. 1987, *Kolpinghuis Nijmegen*, 80/86).
- 26 Si la Directive prévoit que les États membres adoptent et publient, au plus tard le 6 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour s'y conformer (Directive (UE) 2016/680), la Cour de Justice des Communautés européennes a précisé par un arrêt rendu le 18 décembre 1997 dans l'affaire C-129/96, qu'à cet égard, « si les États membres ne sont pas tenus d'adopter ces mesures avant l'expiration du délai de transposition, il résulte de l'application combinée des articles 5, deuxième alinéa, et 189, troisième alinéa, du traité et de la directive elle-même que, pendant ce délai, ils doivent s'abstenir de prendre des dispositions de nature à compromettre sérieusement le résultat prescrit par cette directive » (CJCE, 18 déc. 1997, *Inter-Environnement Wallonie*, 129/96, point 45).
- 27 C'est ainsi que le Conseil d'État a également été amené à reconnaître que « si, pour atteindre ce résultat à l'issue du délai qui leur est imparti dans la directive, les autorités nationales restent seules compétentes pour décider de la forme à donner à l'exécution de ces directives et pour fixer elles-mêmes, sous le contrôle des juridictions nationales, les moyens propres à leur faire produire leurs effets en droit interne, elles ne peuvent légalement prendre, ainsi que l'a précisé la Cour de Justice des Communautés européennes par un arrêt rendu le 18 décembre 1997 dans l'affaire C-129/96, pendant le délai imparti par la directive, des mesures de nature à compromettre sérieusement la réalisation du résultat prescrit par la directive. » (Conseil d'État, 9^e et 10^e SSR, 10 janv. 2001, *France Nature Environnement*, n° 217237)
- 28 **Par conséquent**, en concluant à l'irrecevabilité de la requête, le Conseil d'État priverait Madame In't Veld de la possibilité effective d'exercer pleinement son droit de recours, et contreviendrait à l'application du droit de l'Union.

3. Sur le fond

- 29 **En premier lieu**, concernant l'absence de notification de la vérification, le Premier ministre fait valoir que « *Mme In't Veld soutient de façon très succincte [...] que la CNCTR ne lui a pas notifié sa décision, et que la décision implicite de rejet de sa demande serait insuffisamment motivée et ce faisant illégale* » mais que « *néanmoins, la requérante admet dans son mémoire ampliatif avoir reçu un courrier de la CNCTR en date du 13 septembre 2016* ».

- 30 Le Conseil d'État ne pourra que constater que la requête du 8 septembre 2016 précède chronologiquement la notification de la CNCTR par courrier du 13 septembre 2016. Le courrier du 13 septembre ne pourra donc être pris en compte, celui-ci étant intervenu après le délai imparti à la CNCTR. La seule décision pouvant être prise en compte est la décision implicite de rejet, par définition non motivée.
- 31 **En second lieu**, le Premier ministre avance que le droit à un recours serait « *largement ouvert* » en matière de renseignement et que le présent recours en serait « *la parfaite illustration* ». Cela est d'autant plus contradictoire que l'ensemble de l'argumentation développée par le Premier ministre a précisément pour objectif de refuser à Mme In't Veld le droit à un recours en matière de surveillance internationale.
- 32 Quoiqu'il en soit, le Premier ministre soutient, en substance, que le dispositif mis en place par la Loi Renseignement ne méconnaît pas les exigences posées par la jurisprudence de la Cour EDH et qu'il n'y a pas lieu de contrôler sa conformité au regard du droit de l'Union européenne, notamment en matière de droit à un recours effectif.
- 33 Or, comme il sera de nouveau démontré *infra*, tant la procédure d'autorisation que celle de mise en œuvre des mesures de surveillance internationale au cause, qu'elles précèdent ou succèdent l'entrée en vigueur des lois n° 2015-912 (dite « Loi Renseignement ») et n° 2015-1556 (dite « Loi sur la Surveillance Internationale »), ne respectent les garanties nécessaires à l'exercice du droit à un recours effectif au titre de l'article 13 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (la Convention) et de l'article 47 de la Charte des droits fondamentaux de l'Union européenne (la Charte). Pourtant, de telles garanties sont d'autant plus nécessaires que ces mesures causent une ingérence particulièrement grave dans les droits et libertés protégés au titre de l'article 8 de la Convention et des articles 7 et 8 de la Charte.

3.1. Sur la mise en œuvre du droit de l'Union

- 34 À titre liminaire, il convient de rappeler que la protection des droits reconnus par la Charte doit trouver son plein effet en l'occurrence.²
- 35 Le Premier ministre soutient qu'il n'y a pas lieu de poser de question préjudicielle, demandant ainsi au Conseil d'État de se dispenser d'analyser la conformité du droit français au regard du droit de l'Union. Or, le Conseil d'État n'ignore pas que la question de la surveillance des communications électroniques par les États a récemment fait l'objet d'un arrêt de la grande chambre de la Cour de justice de l'Union européenne (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15). Cette jurisprudence ne peut être ignorée, en ce qu'elle confirme sans ambiguïté que les mesures de surveillance internationale en cause relèvent d'une mise en œuvre du droit de l'Union.

2. Voir la section 2 page 5 du mémoire ampliatif du 13 novembre 2016.

36 **En droit**, des mesures nationales permettant aux autorités l'interception et/ou l'accès aux communications électroniques, ainsi qu'aux données y afférentes, relèvent du champ d'application de la directive 2002/58 (v. par analogie : *Tele 2* précité, points 75 et 76). Plus précisément, la grande chambre de la Cour de justice a décidé :

« En effet, la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par **toutes les personnes** autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques. Comme le confirme le considérant 21 de cette directive, celle-ci vise à **empêcher « tout accès »** non autorisé aux communications, **y compris à « toute donnée afférente à ces communications »**, afin de protéger la confidentialité des communications électroniques. » (point 77) [...]

« Le principe de confidentialité des communications instauré par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, paragraphe 1, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, paragraphe 1, de cette directive [...]. » (point 85)

37 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 à la Charte. Le fait que cette mise en œuvre du droit de l'Union repose sur une exception, fondée sur l'article 15, aux fins notamment de défense de la sécurité nationale, ne saurait soustraire celle-ci du respect de la Charte.³

38 **En l'espèce**, les mesures de surveillance internationale prises antérieurement ou postérieurement à l'entrée en vigueur de la Loi sur la Surveillance Internationale, et notamment celles révélées par *L'Obs* initiées dès 2008, portent également sur des accès aux communications électroniques transmises sur des réseaux de communications électroniques.

39 Dès lors, il ne fait aucun doute que les mesures de surveillance en cause ont pour objet l'accès aux données de connexion et/ou l'interception du contenu des communications sur les réseaux de communications électroniques visés. L'entrave que ces mesures constituent au regard du principe de confidentialité desdites communications est, là encore, évident.

40 **Par conséquent**, les mesures de surveillance internationale en cause doivent

3. Voir la jurisprudence antérieure de la Cour, citée en particulier aux paragraphes 36 et suivants du mémoire ampliatif du 13 novembre 2016.

être conformes au droit de l'Union et notamment à la directive 2002/58 interprétée à la lumière de la Charte.

41 Or, les mesures de surveillance internationale des autorités françaises portent atteinte au contenu essentiel du droit à la vie privée et à la protection des données personnelles (section 3.2). Elles ne sont pas non plus limitées au strict nécessaire, ni soumises à un contrôle préalable (section 3.3 page 11). De plus, les règles qui organisent l'autorisation et le contrôle de telles mesures ne respectent ni les garanties nécessaires à l'exercice effectif d'un droit de recours (sections 3.4 page 17) ni les garanties nécessaires au droit à un procès équitable (section 3.5 page 21).

42 De ce fait, les mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de la Loi sur la Surveillance Internationale doivent être considérées comme des techniques de renseignement mises en place irrégulièrement.

3.2. Sur l'atteinte au contenu essentiel du droit au respect de la vie privée

43 **En droit**, conformément à l'article 52(1) de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit notamment être prévue par la loi et respecter leur contenu essentiel.

44 En ce qui concerne le caractère prévu par la loi, force est de constater que les mesures de surveillance internationale en cause étaient mises en œuvre en l'absence de tout cadre légal cohérent avant l'adoption de la loi éponyme. Ainsi que le relevant le Conseil constitutionnel dans son commentaire à l'occasion de la saisine sur la Loi Renseignement :

« L'activité des services de renseignement s'est longtemps inscrite dans un **environnement para-légal, extra-légal voire a-légal**, la France pouvant être regardée comme « rétive à toute intrusion du pouvoir législatif dans le champ des services de renseignement ». La loi relative au renseignement adoptée définitivement par le Parlement le 24 juin 2015 a pour objet de remédier à cette situation en créant un cadre juridique global et cohérent pour l'action de ces services. » (Conseil constitutionnel, commentaire relatif aux Décisions n^{os} 2015-713 DC et 2015-714 DC du 23 juillet 2015, page 2)

45 En ce qui concerne le contenu essentiel de l'article 7 de la Charte, la Cour de justice retient qu'une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée (voir, CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 94 ; et *a contrario*, CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 39).

46 Un tel accès généralisé au contenu de communications par les autorités a déjà été caractérisé par la grande chambre de la Cour de justice concernant les programmes de collecte de renseignements américains. Ainsi, dans l'arrêt *Schrems*, s'appuyant sur les constats de la Commission européenne, la Cour relevait que les autorités américaines pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers les États-Unis. Pour caractériser le nature généralisée de cet accès aux données, la Commission relevait en particulier que :

« la sphère de sécurité sert également d'interface pour le transfert de données à caractère personnel de citoyens européens, de l'[Union] vers les États-Unis, par les entreprises qui sont tenues de remettre des données aux agences américaines de renseignement dans le cadre de programmes américains de collecte de renseignements ». (cité au point 15 de l'arrêt *Schrems*)

« toutes les entreprises participant au programme PRISM [programme de collecte de renseignements à grande échelle], qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis semblent être certifiées dans le cadre de la sphère de sécurité [...] qui] est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'[Union]. [...] un certain nombre de bases juridiques prévues par la législation américaine permettent la collecte et le traitement à grande échelle des données à caractère personnel stockées ou traitées par des sociétés établies aux États-Unis [...]. » (cité au point 22)

« l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis » (cité au point 25).

47 En somme, l'accès est considéré comme un accès généralisé lorsqu'il constitue une voie pour la collecte et le traitement à grande échelle.

48 **En l'espèce**, il y a tout lieu de considérer que les mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de la Loi Renseignement correspondant à de nombreux égards aux mesures de surveillance internationale pouvant à ce jour être mises en œuvre sur le fondement du chapitre IV du titre V du livre VIII du code de la sécurité intérieure. Ainsi que le relevait le Conseil constitutionnel à l'occasion de l'examen de la Loi Renseignement, celle-ci avait pour objet de créer le cadre juridique pour l'action des services de renseignement (cf. ¶ 44 page précédente).

49 Ainsi pour mesurer l'ampleur des pratiques en cause, il y a lieu de rappeler que l'article L. 854-1 CSI dispose :

« Dans les conditions prévues au présent chapitre, peut être autorisée, aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, la surveillance des communications qui sont émises ou reçues à l'étranger.

« Cette surveillance, qu'elle porte **sur des correspondances ou sur des données de connexion**, est exclusivement régie par le présent chapitre. [...] »

50 Il ne fait donc aucun doute que les mesures de surveillance internationale permettent l'accès au contenu de communications électroniques.

51 En outre, l'article L. 854-2 CSI dispose :

« I.-Le Premier ministre désigne, par une décision motivée, **les réseaux de communications électroniques** sur lesquels il autorise l'interception des communications émises ou reçues à l'étranger, dans les limites fixées à l'article L. 854-1.

« II.-Sur demande motivée des ministres ou de leurs délégués mentionnés au premier alinéa de l'article L. 821-2, le Premier ministre ou l'une des personnes déléguées mentionnées à l'article L. 821-4 peut autoriser l'exploitation **non individualisée** des données de connexion interceptées. [...] »

« III.-Sur demande motivée des ministres ou de leurs délégués mentionnés au premier alinéa de l'article L. 821-2, le Premier ministre ou l'un de ses délégués peut également délivrer une autorisation d'exploitation de communications, ou de seules données de connexion, interceptées.

« L'autorisation désigne :

1. La ou les finalités poursuivies parmi celles mentionnées à l'article L. 811-3;
2. Le ou les motifs des mesures;
3. Les **zones géographiques** ou les organisations, groupes de personnes ou personnes concernés;
4. Le ou les services mentionnés à l'article L. 811-2 en charge de cette exploitation.

« L'autorisation, renouvelable dans les mêmes conditions que celles prévues au présent III, est délivrée pour une durée maximale de quatre mois. »

52 Cet article illustre bien le fait que les mesures de surveillance internationale sont mises en œuvre sur des réseaux entiers, permettent une exploitation non individualisée, et peuvent couvrir des zones géographiques entières (y compris pour l'exploitation du contenu des communications). Dès lors, les mesures de surveillance internationale constituent une voie pour la collecte et le traitement à grande échelle des communications électroniques interceptées. Ce qui induit d'ailleurs que c'est l'ensemble de la population qui risque d'être sujette à ce type de mesures, y compris Madame In't Veld, et que

dès lors, il n'y a pas lieu de considérer que les mesures de surveillance internationale n'ont pas été mises en œuvre à son égard.

53 Compte tenu de la généralité des mesures mises en œuvre, il y a tout lieu de présumer qu'une mesure de surveillance internationale a été mise en œuvre à son égard. C'est alors, comme énoncé *supra* au Premier ministre de démontrer qu'il n'y a pas eu de mesure de surveillance mise en œuvre envers Madame In't Veld.

54 **Par conséquent**, les mesures de surveillance internationale en cause permettant aux services de renseignement français d'accéder de manière généralisée au contenu de communications électroniques. Ces mesures doivent donc être considérées comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée. De telles mesures sont donc prises en violation des articles 7 et 52(1) de la Charte.

55 En tout état de cause, les mesures de surveillance internationale constituent une ingérence dans les droits et libertés reconnus par la Charte et doivent, dès lors, être proportionnées.

3.3. Sur le défaut de limitation au strict nécessaire

56 Quand bien même certaines mesures de surveillance internationale portant sur des données et non sur le contenu des communications ne seraient pas susceptibles de porter atteinte au contenu essentiel du droit au respect de la vie privée, ces mesures constituent une ingérence de vaste ampleur et particulièrement grave (voir par analogie : CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15).

57 Les mesures de surveillance internationale en cause constituent une ingérence qui ne peut donc être justifiée que par des objectifs suffisamment graves, strictement limités et restreints, tout en étant soumis à des règles et des procédures appropriées pour garantir la limitation au strict nécessaire des mesures de surveillance, conformément à la Charte telle qu'interprétée par la Cour de justice. Or, les mesures de surveillance internationale françaises ne sont pas limitées au strict nécessaire.

3.3.1. Sur les objectifs susceptibles de justifier l'interception des communications

58 En premier lieu, mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de Loi sur la Surveillance Internationale ont été mises en œuvre en dehors de tout cadre légal. Ne servant pas d'objectif défini par la loi ces mesures méconnaissent nécessairement les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne en ce qu'elles ne limitent nullement l'interception de communications électroniques à des fins de mesures de surveillance internationale à la poursuite d'objectifs

susceptibles de justifier le caractère particulièrement grave et de vaste ampleur de l'ingérence qu'elles causent.

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

- la sauvegarde de la sécurité nationale (ou la « sûreté de l'État »), la défense et la sécurité publique ;
- la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ;
- les objectifs visés à l'article 13, paragraphe 1, de la directive 95/46, à savoir ceux mentionnés précédemment ainsi que :
 - d) la prévention, la recherche, la détection et la poursuite [...] de manquements à la déontologie dans le cas des professions réglementées ;
 - e) la poursuite d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;
 - f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) ;
 - g) la protection de la personne concernée ou des droits et libertés d'autrui.

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

61 Ainsi, *en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales*, la **lutte contre la criminalité grave est le seul objectif d'intérêt général** susceptible de justifier une mesure d'accès aux communications électroniques, dès lors qu'une telle mesure constitue une ingérence particulièrement grave (point 102 de l'arrêt *Tele2*).

62 **En l'espèce**, les mesures de surveillance internationale mises en œuvre antérieurement à l'entrée en vigueur de la Loi Renseignement ne servent aucun objectif défini par la loi, faute d'encadrement légal.

63 Après l'entrée en vigueur de la Loi Renseignement, les mesures de surveillance internationale sont autorisées aux « fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ». En effet, l'article L. 801-1 dispose en son alinéa 2 que :

« L'autorisation et la mise en œuvre **sur le territoire national** des techniques de recueil de renseignement mentionnées aux chapitres Ier à III du titre V du présent livre ne peuvent être décidées que si :
« [...] 4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article

L. 811-3 ; »

64 Or, les mesures de surveillance internationale en cause — qu'il s'agisse d'accès aux données de connexion ou d'interception des communications d'un réseau — sont bien mises en œuvre sur le territoire national. En effet, comme le révélait l'article de *L'Obs* déjà cité :

« On a bien pensé à espionner à l'abri de cette législation, dans les eaux internationales. Mais on s'est vite rendu compte qu'il était impossible de poser une bretelle au fond de la mer, dit un homme de l'art. On ne sait 'brancher' que sur terre.» [...]

« Une première station clandestine d'interception est mise en service à Marseille le 1er novembre 2008. Le câble visé ? Le SEA-ME-WE 4. Posé par Alcatel trois ans auparavant, il relie la cité phocéenne à Singapour en passant par Annaba, Le Caire et Djeddah. »

65 L'article L. 811-3 dispose que :

« Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux **techniques mentionnées au titre V du présent livre** pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :

1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;

2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;

4° La prévention du terrorisme ;

5° La prévention :

a) Des atteintes à la forme républicaine des institutions ;

b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;

c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;

6° La prévention de la criminalité et de la délinquance organisées ;

7° La prévention de la prolifération des armes de destruction massive »

66 Le Conseil constitutionnel a pu préciser l'interprétation à donner à ces objectifs :

« Considérant qu'en retenant, pour déterminer les finalités énumérées aux 1° à 4°, des définitions faisant référence à certains des intérêts mentionnés à l'article 410-1 du code pénal, le législateur a précisément circonscrit les finalités ainsi poursuivies et n'a pas retenu des

critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ; qu'il en va de même pour les finalités définies au a) du 5°, faisant référence aux incriminations pénales du chapitre II du titre Ier du livre IV du code pénal, de celles définies au b) du 5°, faisant référence aux dispositions de l'article L. 212-1 du code de la sécurité intérieure, de celles définies au c) du 5°, faisant référence aux incriminations pénales définies aux articles 431-1 à 431-10 du code pénal, de celles définies au 6°, faisant référence aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée et de celles définies au 7°, faisant référence aux incriminations pénales définies aux articles L. 2339-14 à L. 2339-18 du code de la défense ; » (Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC, considérant 10)

67 Ainsi, force est de constater que les finalités poursuivies au 5° et 6° de l'article L. 811-3 dépassent le cadre de la lutte contre la criminalité grave. Par exemple, ces finalités convrent la lutte contre le délit défini à l'article 431-9 du code pénal qui consiste à « avoir organisé une manifestation sur la voie publique n'ayant pas fait l'objet d'une déclaration préalable dans les conditions fixées par la loi ». Ce délit est puni de six mois d'emprisonnement et ne peut, dès lors, être considéré comme relevant de la criminalité grave.

68 **En conséquence**, les objectifs poursuivis par les mesures de surveillance internationale mises en œuvre avant ou après l'entrée en vigueur de la Loi Renseignement ne sont pas suffisamment limités.

69 Pour cette raison, déjà, le Conseil d'État doit constater l'illégalité des mesures de surveillance en cause, en ce qu'elles méconnaissent les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne.

3.3.2. Sur l'insuffisance des conditions matérielles et procédurales régissant les mesures de surveillance internationale

70 En second lieu, y compris pour les objectifs susceptibles d'être conformes aux exigences posées par la Cour de justice, les mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de la Loi sur la Surveillance Internationale méconnaissent les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne en ce qu'elles ne sont pas assorties des « conditions matérielles et procédurales » suffisantes pour limiter au strict nécessaire l'ingérence que constituent les mesures de surveillance internationale (*Tele2* point 118).

71 **En droit**, dans l'arrêt *Tele 2*, la Cour de justice a posé les exigences applicables à une réglementation nationale prévoyant l'accès aux données conservées relatives aux communications électroniques. *A fortiori* les exigences suivantes s'appliquent à une mesure nationale ouvrant la voie à l'accès massif aux communications électroniques :

— tout accès à des données de communications électroniques doit porter

sur des personnes pour lesquelles il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective aux intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique (point 119) ;

- tout accès doit être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante (point 125) ;
- les données auxquelles il est accédé doivent être conservées sur le territoire de l'Union (*ibid*).

72 **En l'espèce**, les mesures de surveillance internationale en cause méconnaissent chacune de ces exigences puisqu'aucun cadre procédural n'était défini pour assurer leur mise en œuvre.

73 **En ce qui concerne les personnes faisant l'objet des mesures**, il n'existe aucun élément objectif permettant de considérer que l'ensemble des personnes utilisant un réseau de communications électroniques ouvert au public sont susceptibles d'apporter des éléments objectifs au regard des finalités poursuivies. Au contraire, les interceptions aux fins de surveillance internationale sont susceptibles de porter sur des personnes pour lesquelles il n'existe aucun lien justifiant l'interception de leurs communications électroniques au regard des finalités poursuivies, lesquelles étaient d'ailleurs indéterminées.

74 En pratique, les mesures de surveillance internationale mises en œuvre depuis 2008 concernent l'interception du trafic de câbles sous-marins provenant de pays entiers. Ainsi, en juillet 2015, *L'Obs* révélait que :

L'actuel patron de la commission, Jean-Claude Delarue [sic] , refuse de confirmer publiquement cette procédure classée "secret-défense". D'après nos informations, il a, ces dernières années, donné son feu vert pour l'interception du trafic câble en provenance d'une quarantaine de pays. Ceux du Maghreb : Algérie, Maroc ou Tunisie ; du Moyen-Orient : Iran, Irak, Syrie ou Arabie saoudite ; d'une grande partie de l'Afrique subsaharienne ; et puis, bien sûr, les grands : Russie, Chine, Inde, Etats-Unis aussi. . .

75 Il est par conséquent indéniable que les mesures de surveillance internationale en cause ne délimitent pas suffisamment par des éléments objectifs l'interception des communications des seules personnes pour lesquelles il existerait un lien justifiant l'interception.

76 **En ce qui concerne l'absence de contrôle indépendant de l'autorisation des mesures de surveillance internationale**, la grande Chambre de la Cour de justice a décidé que :

« [...] il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, **subordonné à un contrôle préalable** effectué soit par une juridiction soit par une entité administrative indé-

pendante, et **quela décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités** présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 62 ; voir également, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:ECHR:2016:0112JUD003713814, §§ 77 et 80). » (point 120)

77 Or, force est de constater que les mesures de surveillance internationale mises en œuvre avant ou après l'entrée en vigueur de la Loi Renseignement ou de la Loi sur la Surveillance Internationale ne prévoient aucun contrôle préalable, ni décision d'une autorité indépendante intervenant suite à une demande motivée des autorités.

78 **En ce qui concerne l'exigence de conservation sur le territoire de l'Union**, les documents révélés par Edward Snowden ont permis d'établir l'importance des échanges de données massifs avec les agences de renseignement étrangères, y compris en dehors de l'Union européenne. Fin 2011, la DGSE aurait ainsi signé avec la NSA américaine et les autres agences des « Five Eyes » un memorandum relatif au partage en temps réel de renseignements, mais également de données brutes et une coopération en matière de cryptanalyse, tirés notamment de mesures de surveillance internationale⁴.

79 En octobre 2013, sur la base des documents révélés par Snowden, le journal *Le Monde* avait jeté la lumière sur ces mécanismes de coopération :

De nouvelles pièces, transmises au *Monde* par Edward Snowden, un ancien consultant de la NSA, lèvent, pourtant, le voile sur une autre réalité : celle des liens extrêmement étroits noués par les services secrets français, la Direction générale des services extérieurs (DGSE), avec, d'une part, la NSA et, d'autre part, son équivalent britannique, le GCHQ, soit les deux plus puissantes structures d'interceptions techniques au monde.

Ces nouveaux éléments montrent comment et à quel point, au nom de la lutte antiterroriste, la DGSE a construit et structuré ses échanges avec les Etats-Unis et la Grande-Bretagne. La coopération s'est développée sur le terrain du renseignement technique et humain. Dans le cadre d'un troc, **la décision a ensuite été prise de transférer à la NSA et au GCHQ des stocks massifs de données transitant sur le sol français.**

Ces documents internes à la NSA ou au GCHQ attestent que les décisions inhérentes à la création de ce versement dans un

4. JAUVERT, Vincent. EXCLUSIF. Comment la France écoute (aussi) le monde. In : L'Obs [en ligne]. 1 juillet 2015. [Consulté le 1 juillet 2015]. Disponible à l'adresse : <http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>

vaste pot commun de données privées et publiques françaises se sont prises, en grande partie, au niveau des directeurs des services secrets techniques de ces pays (...).

Selon un haut responsable de la communauté du renseignement en France, ce partage n'est pas exempt de quelques « *cachotteries de part et d'autre* ». Mais, dit-il, la DGSE a approfondi plus encore sa relation avec ses partenaires anglo-saxons, notamment la NSA, à partir de fin 2011 et début 2012, **en adoptant un protocole d'échange de données massif**. La France bénéficie d'une position stratégique **en matière de transport de données électroniques par les câbles sous-marins**. Ce flux d'informations étranger-France, cette « *matière première* » comme la qualifie la NSA dans une note révélée par M. Snowden, fait l'objet d'une **large interception par la DGSE**.

Mais le matériau fourni à la NSA, en grande partie prélevé sur les câbles mais pas seulement, n'est pas uniforme. Les données collectées ont des caractéristiques techniques très variées et complexes. Elles appartiennent à des Français comme à des étrangers. La DGSE peut trier certaines d'entre elles et ainsi préserver des secrets concernant la France, mais elle ne peut pas tout identifier.⁵

80 À titre d'illustration, sur la base d'investigations réalisées par le *Wall Street Journal*, le journal *Le Monde* rapportait à l'époque qu'entre le 10 décembre 2012 et le 8 janvier 2013, 70,3 millions de données téléphoniques collectées en France avaient été transmises par la DGSE à la NSA⁶. Rappelons enfin que c'est dans le cadre d'accords de coopération de même nature que le BND allemand aurait transmis à la NSA des données relatives aux intérêts stratégiques français⁷.

3.4. Sur l'absence d'information de la mesure de surveillance

81 Le Premier ministre avance en substance que le droit à la protection juridictionnelle effective ainsi que le droit au recours ne sont pas remis en cause

5. FOLLOROU, Jacques. La France, précieux partenaire de l'espionnage de la NSA. In : *Le Monde* [en ligne]. 29 novembre 2013. [Consulté le 12 mai 2015]. Disponible à l'adresse : http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html.

6. FOLLOROU, Jacques. Surveillance : la DGSE a transmis des données à la NSA américaine. In : *Le Monde.fr* [en ligne]. 30 octobre 2013. [Consulté le 16 mars 2016]. Disponible à l'adresse : http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

7. FOLLOROU, Jacques. La France avait été alertée d'une menace imminente. In : *Le Monde* [en ligne]. 17 novembre 2015. [Consulté le 17 novembre 2015]. Disponible à l'adresse : http://www.lemonde.fr/attaques-a-paris/article/2015/11/17/la-france-avait-ete-alertee-d-une-menace-imminente_4811797_4809495.html.

de manière disproportionnée par l'absence d'information à destination de la personne concernée par la mise en œuvre d'une mesure de surveillance secrète.

82 Or, les mesures de surveillance internationale mises en œuvre avant l'entrée en vigueur de la Loi sur la Surveillance Internationale portent atteinte au droit au respect de la vie privée et au droit au recours effectif garantis par les articles 8 et 13 de la Convention, ainsi qu'à l'article 47 de la Charte, en tant qu'elle ne garantissent pas une possibilité effective de contester rétrospectivement les techniques de renseignement mises en œuvre, en raison de l'absence d'information satisfaisante des personnes concernées.

83 **En premier lieu et en droit**, aux termes de l'article 8 de la Convention :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

« 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

84 En outre, et encore en droit, selon les termes de l'article 13 de la Convention :

« Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

85 À ce titre, la Cour européenne des droits de l'homme (Cour EDH) estime que :

« l'article 13 de la Convention garantit l'existence en droit interne d'un recours permettant de se prévaloir des droits et libertés de la Convention tels qu'ils y sont consacrés. Cette disposition a donc pour conséquence d'exiger un recours interne habilitant à examiner le contenu d'un "grief défendable" fondé sur la Convention et à offrir le redressement approprié »

(Cour EDH, g^{de} ch., 13 déc. 2012, *De Souza Ribeiro c. France*, n° 22689/07, § 78).

86 En somme, le droit au recours effectif ainsi conçu a pour objet de permettre la protection d'autres droits conventionnels, tels que le droit au respect de la vie privée, dès lors qu'il existe une ingérence au sein de l'un de ces droits. En effet, pour la juridiction européenne :

« quand un État instaure une surveillance secrète dont les personnes contrôlées ignorent l'existence et qui demeure dès lors inattaquable,

l'article 8 [...] pourrait dans une large mesure être réduit à néant. Dans une telle situation, il se peut qu'un individu soit traité d'une façon contraire à l'article 8 [...], voire privé du droit garanti par cet article [...], sans le savoir et partant sans être à même d'exercer un recours au niveau national ou devant les organes de la Convention. » (Cour EDH, Plén., 6 sept. 1978, *Klass c. All.*, n° 5029/71, § 36).

- 87 Face à une telle situation, la Cour estime avec force qu'« il importe de s'assurer que le caractère secret de pareilles mesures ne conduise pas à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités nationales et de la Cour » (Cour EDH, 4^e sect., 18 mai 2010, *Kennedy c. R-U*, n° 26839/05, § 124).
- 88 À cet égard, tant la Cour EDH que la Cour de justice ont eu l'occasion d'insister sur la nécessité que les personnes concernées par une mesure de surveillance secrète bénéficient d'une information appropriée de nature à permettre l'exercice des voies de recours, lorsqu'une telle information n'est plus susceptible de remettre en cause l'efficacité de la mesure en cause.
- 89 Dans l'arrêt *Roman Zakharov c. Russie* du 4 décembre 2015, la grande chambre de la Cour européenne des droits de l'homme a rappelé au sujet des mesures de surveillance secrète que « lorsque la surveillance a cessé, la question de la notification a posteriori de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance » (Cour EDH, g^{de} ch., 4 déc. 2015, *Zakharov c. Russie*, n° 47143/06, § 234).
- 90 De fait, « la personne concernée [par la surveillance] ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (Klass et autres, précité, § 57, et Weber et Saravia, décision précitée, § 135) ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure (Kennedy, précité, § 167). » (Ibid.).
- 91 C'est notamment à ce titre que dans cette affaire, et à l'unanimité, la grande chambre a constaté une violation de l'article 8, en lien avec l'article 13 de la Convention, aux motifs que « le droit russe n'offre pas de recours effectif à une personne qui pense avoir fait l'objet d'une surveillance secrète. En privant la personne visée par l'interception de la possibilité effective de contester rétrospectivement des mesures d'interception, le droit russe néglige d'offrir une importante garantie contre l'utilisation indue de mesures de surveillance secrète » (Ibid. § 300).
- 92 Pour parvenir à cette conclusion, la Cour a souligné qu'« en Russie **les personnes dont les communications ont été interceptées ne reçoivent à aucun moment ni en aucune circonstance notification de cette mesure** » (§ 289). En outre, même s'il a « appris d'une manière ou d'une autre que ses communications ont été interceptées », « le sujet

de l'interception **n'a pas de droit d'accès aux documents relatifs à l'interception de ses communications** ; il peut, au mieux, recevoir "des informations" sur les données recueillies ». Et en tout état de cause, « seules des informations ne contenant pas de secrets d'État peuvent être divulguées à la personne visée par l'interception », sachant « qu'en droit russe les informations relatives aux installations utilisées pour la mise en œuvre de mesures opérationnelles d'investigation, aux méthodes employées, aux agents qui sont intervenus et aux données recueillies constituent un secret d'État » (§ 290).

93 Dans ces conditions, la Cour conclut à l'unanimité à la violation de l'article 13 en ce que « l'effectivité d[es éventuels] recours est donc compromise par l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception, *et* par l'inexistence d'une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations sur les interceptions. » (§ 298)

94 **En second lieu, en droit**, aux termes de l'article 47 de la Charte :

« Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter »

95 En matière d'accès aux données de connexion, la grande chambre de la Cour de justice fait de l'information des personnes concernées, une condition de fait nécessaire à l'exercice du droit de recours et à la protection juridictionnelle effective. Le raisonnement suivi dans l'arrêt *Tele 2* précité est pleinement transposable aux mesures de surveillance secrète concernant les données et le contenu des communications transmises sur un réseau de communications électroniques :

« il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informant les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, **cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours**, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits (voir, par analogie, arrêts du 7 mai 2009, *Rijkeboer*, C553/07, EU:C:2009:293, point 52, ainsi que du 6 octobre 2015, *Schrems*, C362/14, EU:C:2015:650, point 95). » (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, point 121)

96 Il peut être noté que la circonstance que la mesure nationale soit prise pour

les intérêts de la sécurité nationale ne saurait soustraire les autorités du respect de l'exigence posée à l'article 15 de la directive 2002/58 ; puisque celui-ci vise précisément la défense de la sécurité nationale.

97 En somme, une législation nationale ne prévoyant pas l'information des personnes concernées lorsque cela n'est pas susceptible de compromettre les enquêtes menées par les autorités porte donc une atteinte disproportionnée au droit des personnes d'exercer un recours tel que prévu notamment à l'article 47 de la Charte.

98 **En l'espèce**, aucune information satisfaisante des personnes concernées n'était prévue par le droit français quant aux mesures de surveillance antérieures ou postérieures à l'entrée en vigueur de la Loi sur la Surveillance Internationale.

99 En l'occurrence, l'existence du système d'interception massif mis en place par la DGSE depuis 2008 a été révélée par la presse. Ces révélations n'ont d'ailleurs fait l'objet d'aucune contestation de la part du gouvernement.

100 Or, ces mesures de surveillance internationale n'ont fait l'objet d'aucune communication à destination des personnes concernées, même lorsqu'une telle communication n'était pas susceptible de compromettre les enquêtes menées par ces autorités.

101 **Par conséquent**, en n'ayant pas informée la requérante de la mise en œuvre d'une mesure de surveillance internationale dès le moment où cette communication n'était pas susceptible de compromettre les nécessités des objectifs poursuivis ; l'État français a privée de fait Madame In 't Veld de la possibilité effective d'exercer pleinement son droit de recours.

3.5. Sur l'absence de procès équitable et de protection juridictionnelle effective

102 Le Premier ministre défend que la possibilité de saisir le CNCTR en matière de surveillance internationale suffirait à donner une possibilité effective de contestation des mesures de surveillance. Pourtant, la procédure de vérification ne répond pas aux exigences de protection juridictionnelle posées par la Cour de justice.

103 **En droit**, aux termes de l'article 47 de la Charte :

« Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter »

104 Si, la protection juridictionnelle peut connaître des aménagements pour tenir compte des considérations légitimes de sûreté de l'État, les règles de

procédure doivent néanmoins opérer une conciliation entre ces considérations d'une part, et la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, tels que le droit d'être entendu ainsi que le principe du contradictoire, d'autre part (CJUE, g^{de} ch., 4 juin 2013, ZZ, C-300/11, point 57). Plus encore, la Cour impose, s'agissant des « exigences auxquelles doit répondre le contrôle juridictionnel de l'existence et du bien-fondé des raisons invoquées par l'autorité nationale compétente au regard de la sûreté de l'État membre concerné, [...] qu'un juge soit chargé de vérifier si ces raisons s'opposent à la communication des motifs précis et complets sur lesquels est fondée la décision en cause ainsi que des éléments de preuve y afférents » (*ibid.* point 60). Partant,

« il incombe à l'autorité nationale compétente d'apporter, conformément aux règles de procédure nationales, la preuve que la sûreté de l'État serait effectivement compromise par une communication à l'intéressé des motifs précis et complets qui constituent le fondement [de la décision mise en cause]. Il en découle qu'il n'existe pas de présomption en faveur de l'existence et du bien-fondé des raisons invoquées par une autorité nationale [...] et que] le juge national compétent doit procéder à un examen indépendant de l'ensemble des éléments de droit et de fait invoqués par l'autorité nationale compétente et il doit apprécier, conformément aux règles de procédure nationales, si la sûreté de l'État s'oppose à une telle communication »
(CJUE, g^{de} ch., 4 juin 2013, ZZ, C-300/11, points 60 et 62)

- 105 En tout état de cause, au titre de l'article 47 de la Charte, la Cour de justice exige des États qu'ils garantissent la « protection juridictionnelle effective tout en limitant les ingérences éventuelles dans l'exercice de ce droit au strict nécessaire » (*ibid.* point 64).
- 106 En outre, le droit reconnu à l'article 47 a une portée plus étendue que l'article 6§1 de la Convention, lequel prévoit :

« Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice ».

- 107 Certes, dans son arrêt *Kennedy c. Royaume-Uni* relatif à des mesures de surveillance secrète, la Cour européenne des droits de l'homme a souligné qu'elle « souscri[va]it à la thèse du Gouvernement [britannique] selon laquelle la divulgation de documents écrits et la désignation d'avocats spéciaux étaient impossibles en ce qu'elles auraient empêché la réalisation de l'objectif poursuivi, à savoir la préservation du secret sur la réalisation d'interceptions » (Cour EDH, 4^e sect., 18 mai 2010, *Kennedy c. R-U*, n° 26839/05, § 187).
- 108 Mais si la Cour a jugé que la procédure interne ainsi organisée ne violait par l'article 6 de la Convention, ce n'est qu'après avoir relevé que « lorsque [la Commission des pouvoirs d'enquête (Investigatory Powers Tribunal)] donne gain de cause à un plaignant, il lui est loisible de divulguer les documents et les informations pertinents en application de l'article 6.4 de son règlement » (*ibid.* § 167). Soit une possibilité qui représente un minimum nécessaire mais pas suffisant, pourtant absent dans la procédure de vérification.
- 109 **En l'espèce**, la présente procédure méconnaît chacune de ces exigences.

3.5.1. Sur la méconnaissance du principe du contradictoire

- 110 Les conditions dans lesquelles les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative (CJA) ont institué le contrôle juridictionnel du Conseil d'État concernant les techniques de renseignement méconnaissent les exigences du droit au recours effectif et au procès équitable, tout particulièrement le principe corrélatif du contradictoire.
- 111 Et ce, puisqu'à rebours complet des exigences de la Cour de justice de l'Union européenne, ce n'est pas la juridiction compétente mais l'une des parties à l'instance – en l'occurrence, l'administration – qui détermine l'étendue des pièces susceptibles d'être débattues contradictoirement.
- 112 En effet, il y a lieu de souligner que l'article L. 773-6 CJA dispose que :
- « Lorsque la formation de jugement constate l'absence d'illégalité dans la mise en œuvre d'une technique de recueil de renseignement, la décision indique au requérant ou à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique. Elle procède de la même manière en l'absence d'illégalité relative à la conservation des renseignements. »

- 113 En outre, les dispositions de l'article L. 773-7 CJA prévoient que :

« Lorsque la formation de jugement constate qu'une technique de recueil de renseignement est ou a été mise en œuvre illégalement ou qu'un renseignement a été conservé illégalement, elle peut annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés.

« **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. Saisie de conclusions en ce sens lors d'une requête concernant la mise en

œuvre d'une technique de renseignement ou ultérieurement, elle peut condamner l'Etat à indemniser le préjudice subi.

« 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. »

114 Enfin, l'article R. 773-24 CJA, alinéa 1^{er} dispose que :

« Dans les cas où les débats sont susceptibles de porter sur des informations protégées par le secret de la défense nationale, ou de confirmer ou infirmer la mise en œuvre d'une technique de renseignement à l'égard du requérant, ou de révéler des éléments contenus dans le traitement de données, ou si le requérant figure ou non dans le traitement, le requérant est invité à présenter ses observations avant les conclusions du rapporteur public et, après les avoir formulées, à se retirer. Le défendeur, les représentants de la Commission nationale de contrôle des techniques de renseignement et les autres personnes présentes se retirent également. »

115 En somme, le secret de la défense nationale peut faire radicalement obstacle au débat contradictoire devant le Conseil d'État.

116 En l'absence de toute définition légale sur ce qui relève matériellement du secret défense, tout au plus est-il possible d'identifier une doctrine de la « stratégie de défense nationale » (en ce sens, v. Bigo Didier et al., « National security and secret evidence in legislation and before the courts : Exploring the challenges », European Parliament Publications Office, 2014, annexe 5, p. 99). La synthèse d'une telle stratégie peut être trouvée à l'article L. 1111-1 du code de la défense, lequel dispose que :

« La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter. »

117 Il est d'ailleurs significatif que l'article L. 1111-1 alinéa 2 du code de la défense souligne que « l'ensemble des politiques publiques concourt à la sécurité nationale ». Ainsi, aucune politique ne peut être raisonnablement exclue de la lettre de l'article L. 1111-1 du code de la défense.

118 Il en est d'autant plus ainsi que la notion de « sécurité nationale » est elle-même définie de façon extrêmement vaste comme étant, selon l'arrêt du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale,

« la protection du secret concerne tous les domaines d'activité relevant de la défense et de la sécurité nationale : politique, militaire, diplomatique, scientifique, économique, industriel ».

119 Ensuite, et d'autre part, aux termes de l'article 413-9 du code pénal, les éléments qui « présentent un caractère de secret de la défense nationale » sont ceux « qui ont fait l'objet de mesures de classification », laquelle dépend de la seule décision des autorités administratives et ministérielles elles-mêmes (v. l'article R. 2311-6 du code de la défense).

120 Et ce, sans contrôle juridictionnel, ni même un véritable contrôle parlementaire, lequel est extrêmement limité notamment compte tenu de l'opposabilité du secret défense aux commissions d'enquêtes parlementaires (v. l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et Cons. constit. décision n° 2001-456 DC du 27 décembre 2001, cons. 42 et s.). En outre, si la procédure de déclassification prévue par l'article L. 2312-4 du code de la défense fait certes intervenir la Commission consultative du secret de la défense nationale (CCSDN), les avis rendus par celle-ci ne s'imposent pas aux autorités administratives.

121 Dans ces conditions, il apparaît qu'à l'occasion d'un recours initié sur le fondement des articles L. 773-1 à L. 773-8 CJA, l'administration peut elle-même, et sans contrôle aucun, exclure totalement certaines informations du débat contradictoire en les plaçant sous le sceau du secret de la défense nationale, et ce, en méconnaissance flagrante tant (i) de l'obligation d'apporter la preuve que la sûreté de l'État serait effectivement compromise par une communication à la partie au procès, que (ii) de l'exigence selon laquelle le juge national compétent doit pouvoir procéder à un examen indépendant de l'ensemble des éléments de droit et de fait invoqués pour apprécier si la sûreté de l'État s'oppose à une telle communication, conformément à la jurisprudence *ZZ* de la CJUE (rappelée plus haut, ¶ 104 page 22).

122 Il en est d'autant plus ainsi que, corrélativement, le législateur a totalement manqué de prévoir des mesures efficaces pour atténuer l'atteinte ainsi portée à ces droits et exigences.

3.5.2. Sur l'absence de dispositif prévu pour garantir l'accès du requérant ou, à tout le moins, de son représentant aux pièces protégées par le secret défense

123 Enfin, et corrélativement, les dispositions des articles L. 773-1 à L. 773-8 CJA ont méconnu les exigences du droit à un recours effectif faute d'avoir prévu un ensemble de mesures susceptibles de contrebalancer efficacement l'accès privilégié à un ensemble de documents protégés par le secret de la défense nationale dont dispose l'administration.

124 En effet, ainsi que cela a été démontré précédemment, à la différence de l'administration qui dispose de l'ensemble des éléments du dossier concernant la technique de renseignement utilisée, le requérant est quant à lui dépourvu

de tout accès aux éléments les plus essentiels, jusqu'à la jurisprudence spécifique du Conseil d'État en ce domaine puisque seule l'administration pourra l'apprécier par recoupement à l'aune des mesures qui auront été annulées ou au contraire entérinées au terme du contrôle juridictionnel.

125 En somme, le requérant et son éventuel représentant se trouvent dépourvus des moyens indispensables à l'exercice effectif de leur recours contre une mesure de surveillance dont ils ne peuvent même pas apprécier l'ampleur et la teneur.

126 Ainsi, bien au-delà des dispositions de l'article L. 773-3 du code de la justice administrative qui prévoient que « les exigences de la contradiction mentionnées à l'article L. 5 sont adaptées à celles du secret de la défense nationale », il apparaît que ces adaptations affectent la substance même des principes du contradictoire et de l'égalité des armes jusqu'à les réduire à néant.

127 Pourtant, il était loisible au législateur d'adopter des mesures susceptibles de compenser une telle rupture de ces principes garantis au titre de l'article 47 de la Charte.

128 Le droit comparé révèle ainsi qu'il est parfaitement possible de mettre en place un système dédié à une représentation plus efficace des justiciables dans les matières, comme le renseignement, où une atteinte au secret de la défense nationale peut conduire à une adaptation de la procédure.

129 Il en va ainsi des procédures juridictionnelles de supervision des activités de renseignement instituées au Royaume-Uni par l'article 6 du *Justice and Security Act* de 2013, où les justiciables sont représentés par des avocats « spéciaux ».

130 Le rôle et les pouvoirs de tels avocats sont résumés comme suit par les auteurs d'une étude réalisée à la demande du Parlement européen :

« Les avocats spéciaux sont des juristes habilités au secret qui sont autorisés à participer à des procédures fermées et à représenter les requérants. Les avocats spéciaux diffèrent des avocats normaux représentant les requérants. Les avocats spéciaux sont autorisés à révéler à leurs clients un résumé simplifié ou un aperçu des éléments de renseignement utilisés dans le cadre d'audiences secrètes, tout en gardant les détails secrets. Les avocats spéciaux doivent défendre les intérêts de ceux qu'ils représentent et peuvent contester la production de certains éléments sur le fondement qu'elle violerait le procès équitable, mais ils ne peuvent pas échanger avec le requérant sans la permission du Gouvernement et ne peuvent jamais révéler de preuves gardées secrètes. » (Traduction libre de « National Security and Secret Evidence in Legislation and before the Courts : Exploring the Challenges », 10 décembre 2014, étude réalisée à la demande du LIBE Committee).

131 Certes, l'institution de tels avocats spéciaux n'est pas incontestable et

est même ouvertement critiquée, notamment en ce que « l'utilisation des procédures secrètes peut empêcher les requérants d'avoir connaissance de toutes les allégations qui sont faites à leur encontre, ce qui a été critiqué en ce que les parties ne seraient plus sur un pied d'égalité » (Traduction libre de J. Jackson, « Justice, Security and the Right to a Fair Trial : Is the Use of Secret Evidence Ever Fair ? », in Public Law, 2013, 720-736, cité in id., p. 23).

132 Néanmoins, l'existence même d'un tel dispositif démontre à tout le moins qu'il est possible de réduire le déséquilibre considérable de la procédure au détriment du requérant à qui est parfaitement interdit tout accès aux éléments classés comme relevant de la sécurité nationale.

133 Enfin, la seule circonstance que, selon les dispositions de l'article L. 773-5 CJA, le juge compétent puisse soulever tout moyen d'office ne saurait compenser un déséquilibre si grand.

134 En définitive, les dispositions des articles L. 773-1 à L. 773-8 CJA portent atteinte de manière disproportionnée aux droits et principes garantis par l'article 47 de la Charte, ainsi qu'à l'article 6§1 de la Convention.

3.6. Questions préjudicielles

135 Si le Conseil d'État devait douter des conclusions précédentes, il lui reviendrait nécessairement de renvoyer à la Cour de justice les questions préjudicielles suivantes :

« L'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8, 47 et 52, paragraphe 1, de la Charte des droits fondamentaux doivent-ils être interprétés comme autorisant la mise en œuvre de mesures de surveillance des communications en dehors de tout cadre légal, définissant les conditions de leur mise en œuvre ainsi que les conditions de contrôle de leur mise en œuvre ? »

« L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à prévoir qu'en qualité de partie à une instance juridictionnelle relative à une technique de surveillance, les autorités d'un État puissent exclure totalement certaines informations du débat contradictoire en les plaçant – sans contrôle aucun – sous le sceau du « secret de la défense nationale », le tout sans aucune mesure susceptible de réduire efficacement de l'atteinte au droit à un recours effectif ainsi créée ? »

Par ces motifs, et tous autres à produire, déduire, suppléer, au besoin même d'office, la requérante persiste dans les conclusions de ses précédentes écritures et conclut de surcroît à ce que le Conseil d'État :

À titre subsidiaire

- DISE MADAME IN 'T VELD RECEVABLE au titre de l'article L. 773-1 d'un recours formé en application du 1^o de l'article L. 841-1 du code de la sécurité intérieure en ce qu'il n'est pas démontré que la totalité des mesures de surveillance internationale en cause ont continué à être mises en œuvre au-delà du 2 décembre 2015 ;
- PROCÈDE ou fasse procéder à la vérification des mesures de surveillance et d'exploitation ou conservation des renseignements collectés par la DGSE depuis 2008 dont il n'est pas démontré que la mise en œuvre de la totalité de ces mesures aurait continué au-delà du 2 décembre 2015 ;
- CONSTATE que les techniques de recueil de renseignement en cause ont été mises en œuvre en violation de la loi, de la Constitution du droit de l'Union européenne et de la Convention européenne des droits de l'Homme ;
- ORDONNE qu'il soit procédé à la destruction des renseignements me concernant.

En tout état de cause

- SAISISSE la Cour de justice de l'Union européenne des questions préjudicielles suivantes (ou toute autre formulation qu'il voudra bien lui substituer) :

« L'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8, 47 et 52, paragraphe 1, de la Charte des droits fondamentaux doivent-ils être interprétés comme autorisant la mise en œuvre de mesures de surveillance des communications en dehors de tout cadre légal, définissant les conditions de leur mise en œuvre ainsi que les conditions de contrôle de leur mise en œuvre ? »

« L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à prévoir qu'en qualité de partie à une instance juridictionnelle relative à une technique de surveillance, les autorités d'un État puissent exclure totalement certaines informations du débat contradictoire en les plaçant – sans contrôle aucun – sous le sceau du « secret de la défense nationale », le tout sans aucune mesure susceptible de réduire efficacement de l'atteinte au droit à un recours effectif ainsi créée ? »

Le 14 mars à Paris,

Hugo ROY

AVOCAT AU BARREAU DE PARIS

TABLE DES JURISPRUDENCES

CJCE, 6^e, 8 oct. 1987, *Procédure pénale contre Kolpinghuis Nijmegen BV.*, 80/86

CJCE, 18 déc. 1997, *Inter-Environnement Wallonie ASBL contre Région wallonne*, 129/96

CJUE, g^{de} ch., 4 juin 2013, *ZZ c. Secretary of State for the Home Department*, C-300/11

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

CJUE, g^{de} ch., 6 oct. 2015, *Maximilian Schrems contre Data Protection Commissioner*, C-362/14

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

Conseil constit., 23 juill. 2015, *Loi relative au renseignement*, 2015-713 DC

Conseil d'État, 9^e et 10^e SSR, 10 janv. 2001, *France Nature Environnement*, n° 217237

Conseil d'État, form. spé., 19 oct. 2016, *M. A... D...*, n° 396958

Cour EDH, Plén., 6 sept. 1978, *Klass et autres c. Allemagne*, n° 5029/71

Cour EDH, 4^e sect., 18 mai 2010, *Kennedy c. Royaume-Uni*, n° 26839/05

Cour EDH, g^{de} ch., 13 déc. 2012, *De Souza Ribeiro c. France*, n° 22689/07

Cour EDH, g^{de} ch., 4 déc. 2015, *Roman Zakharov c. Russie*, n° 47143/06