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

Conseil d'État
Section du contentieux
N° 404012

Mémoire en réplique

POUR

Sophia Helena in 't Veld
[censuré]

CONTRE

La décision de refus de notification par la Commission nationale de contrôle des techniques de renseignement (CNCTR) et la décision implicite de la CNCTR de ne pas saisir le Conseil d'État en application de l'alinéa 5 de l'article L. 854-9 du code de la sécurité intérieure ;
Toutes décisions d'autorisation et/ou de contrôle des mesures de surveillance internationale initiées depuis 2008 (notamment révélées par la presse depuis 2015) et concernant la requérante.

TABLE DES MATIÈRES

DISCUSSION

1 Dans l'instance n° 404012, 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.

1. Sur l'incompétence de la formation spécialisée

2 A titre liminaire, la requérante soulève l'incompétence de la formation spécialisée pour juger du présent recours en excès de pouvoir et demande la réaffectation à une formation normale du Conseil d'État (qui pourrait, le cas échéant, transmettre à la juridiction compétente pour connaître des décisions attaquées).

3 Les articles L. 773-1 et suivants du code de justice administrative (CJA) relatifs au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État donne compétence à la formation spécialisée du Conseil d'État pour les requêtes présentées sur le fondement des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure (CSI).

4 Le présent recours ne s'inscrivant pas dans le cadre des procédures spéciales prévues par le livre VIII CSI, il n'y a aucune raison pour que la formation spécialisée créée par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement (ci-après, la « Loi Renseignement ») soit compétente en l'espèce. La présente affaire devrait donc être jugée par une formation normale du Conseil d'État.

5 Loin d'être une simple formalité de réaffectation, cette question est d'autant plus importante que la procédure appliquée par la formation spécialisée déroge au droit commun en matière de contrôle juridictionnel et de principe de contradictoire. A titre d'exemple, dans certaines circonstances, la requérante devrait se retirer des débats avant même d'avoir pu entendre les conclusions du rapporteur public (article R. 773-24, al. 1er CJA). [1]

1. Sur les nombreuses dérogations de la procédure de la formation spécialisée, voir le mémoire en réplique du 14 mars 2017 dans l'affaire n° 404013, points 109 et s., p. 23 et s.

2. Sur la recevabilité de la requête

6 La recevabilité de la requête doit être admise à double titre, en ce qu'elle constitue un recours pour excès de pouvoir et que, conformément à la jurisprudence du Conseil d'État, la portée d'un tel recours doit recevoir en l'espèce une application large ; mais également en ce que les dispositions de l'article L. 854-9 ne sont pas applicables à la totalité des mesures de surveillance internationale.

7 **En premier lieu,** le Premier ministre soutient que le recours de Madame In 't Veld serait irrecevable, en citant à l'appui une décision de la formation spécialisée du Conseil d'État (Conseil d'État, form. spé., 19 oct. 2016, *B... A...*, n° 397623). Or, cette décision concerne l'irrecevabilité d'une procédure de vérification, elle est donc sans incidence sur l'interprétation de la recevabilité d'un recours tel que celui engagé en l'espèce, dirigé contre une série de décisions de l'administration.

8 En effet, la procédure de vérification a pour objectif de faire vérifier qu'aucune technique de renseignement n'est mise en œuvre de manière illégale, même lorsqu'une personne ne dispose d'aucun élément. Or, tel n'est pas le cas en l'espèce, puisque Madame In 't Veld dispose d'éléments multiples, révélés notamment par l'article de *L'Obs* déjà cité, sur la mise en œuvre de mesures de surveillance internationale en dehors de tout cadre légal suffisant (cf. Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC, cons. 78). De telles mesures procèdent nécessairement de l'existence d'une ou plusieurs décisions de l'administration (et notamment la décision de la CNCTR de considérer que de telles mesures ne sont pas illégales et faisant ainsi une erreur manifeste d'appréciation).

9 Le présent recours désigne en premier lieu les décisions de la CNCTR car elles sont les seules pouvant être identifiées par la requérante. Ce recours ne doit néanmoins pas être vu comme limité à ces seules décisions. Il porte bien sur l'ensemble des décisions d'autorisation et/ou de contrôle des mesures de surveillance internationale initiées depuis 2008 et révélées par la presse et concernant la requérante Madame In 't Veld. Que l'article L. 854-9 CSI limite les recours pouvant être engagés devant la formation spécialisée n'empêche en rien, contrairement aux dires du Premier ministre, à d'autres procédures d'exister. Cela vaut tout particulièrement pour les mesures de surveillance internationale mises en œuvre et ayant cessé avant l'entrée en vigueur de la Loi sur la Surveillance Internationale.

2.1. Sur la portée matérielle du recours

10 Le Premier ministre prétend que le présent recours devrait être regardé « comme tendant à la mise en œuvre du contrôle prévu à l'article L. 854-9 du CSI. » Cette interprétation est totalement infondée. Madame In 't Veld n'ignore pas que les dispositions de l'article L. 854-9 CSI ne donnent aucun moyen à un individu de saisir la formation spécialisée du Conseil d'État,

puisque cela est expressément rappelé dans le mémoire ampliatif (cf. point 13 page 3)

11 Comme indiqué, le présent recours est dirigé contre la seule décision administrative qui a pu être identifiée, c'est-à-dire le refus implicite de la CNCTR de mettre fin à l'illégalité patente des mesures de surveillance internationale en cause ou de saisir le Conseil d'État comme il en a le pouvoir (cf. section 2 page 2 du mémoire ampliatif). Néanmoins, ce recours doit être vu comme portant sur l'ensemble des mesures de surveillance secrètes qui par leur nature même ne peuvent être désignées par la requérante. En effet, la lecture du mémoire ampliatif ne laisse place à aucun doute sur le fait que la requérante vise une série de décisions administratives relatives à ces mesures de surveillance secrètes (cf. point 19 page 4). Madame In 't Veld rappelle à ce titre que, si le Premier ministre reproche à Madame In 't Veld de ne pas correctement identifier la décision à attaquer, cela résulte entièrement de son propre fait — c'est-à-dire du caractère secret des décisions de mettre en œuvre le système de la DGSE depuis 2008 — dont on ignore encore aujourd'hui la forme légale que celle-ci revêt exactement (voir notamment Conseil d'État, 8e chambre, 18 nov. 2016, *LQDN [Décret non publié sur les activités de surveillance internationale]*, no 393080).

12 Or, les mesures en cause, dont **l'existence n'est aucunement contestée**, ont nécessairement fait l'objet d'une autorisation administrative. Le caractère inconstitutionnel de celle-ci se déduit nécessairement de la décision du Conseil constitutionnel déjà évoquée (cf. section 2 page 6 du mémoire ampliatif).

13 Le Conseil d'État doit nécessairement, conformément à sa jurisprudence, donner une interprétation large de la décision attaquée — d'autant plus lorsque l'identification de la décision est rendue impossible par le caractère secret des décisions d'autorisation des mesures internationales. Le Conseil d'État, qui n'est pas tenu par la qualification que la requérante ait pu en donner, devra qualifier la décision pertinente aux fins de donner plein effet au présent recours, seul possible de mettre fin à l'illégalité patente des mesures en cause.

14 En effet, comme l'explique Mme la Présidente Pascale Fombeur, « *La portée de cette règle sévère est cependant limitée par le pouvoir que le juge administratif se reconnaît d'interpréter les conclusions dont il est saisi, avec d'autant plus de libéralisme que la formulation maladroite lui paraît trahir l'intention réelle de l'auteur de la requête. Et, en règle générale, cette interprétation est faite dans un sens bienveillant (CE, sect., 6 mai 1970, Synd. national du cadre secrétaire-comptable de la Banque de France, Rec. CE, p. 306 ; 4 juin 1976, Desforets, ibid., p. 307 ; 3 nov. 1976, Aufaure, ibid., p. 465).* »[2]

15 Et si les requérants doivent normalement identifier formellement la décision qu'ils entendent attaquer et s'ils doivent en principe joindre cette décision au recours qu'ils introduisent devant le juge administratif, il est acquis qu'en l'espèce cette production est impossible, dès lors que l'acte administratif

2. Répertoire de contentieux administratif, Dalloz, item *Requête*

dont l'annulation est demandé est un acte non publié mais dont l'existence n'est nullement contestée.

16 Enfin, il doit être noté à cet égard que la CNCTR « est subrogée dans les droits et obligations de la Commission nationale de contrôle des interceptions de sécurité » (article 7 du décret n° 2015-1186 du 29 septembre 2015 relatif à l'organisation administrative et financière de la Commission nationale de contrôle des techniques de renseignement). Ainsi, le champ des mesures attaquées ne saurait être limité dans le temps à celles postérieures à la création de la CNCTR.

17 **En second lieu,** le Premier ministre soutient que le recours de Madame In 't Veld serait irrecevable, en citant à l'appui une décision de la formation spécialisée du Conseil d'État (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 la recevabilité du recours pour excès de pouvoir contre les décisions relatives aux mesures de surveillance internationale antérieures à la loi n° 2015-1556 (dite « Loi sur la Surveillance Internationale »).

2.2. Sur le caractère inapplicable des dispositions de l'article L. 854-9 CSI

18 **En droit,** l'article L. 854-9 CSI tel qu'interprété par le Conseil constitutionnel prive toute personne du droit de saisir un juge pour contester les mesures régies par la Loi sur la Surveillance Internationale.

19 Or, 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 œuvre** 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 œuvre après**. »

20 La solution retenue par la formation spécialisée du Conseil d'État est 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**.

21 Le Premier ministre le reconnaît d'ailleurs explicitement lorsqu'il admet (en

page 3 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* ».

22 C'est donc par une lecture erronée de la décision *M. A... D...* précitée que le Premier ministre conclut que le recours pour excès de pouvoir portant sur la période antérieure à l'entrée en vigueur de la Loi sur la Surveillance Internationale ne pourrait qu'être rejeté.

23 **En l'espèce,** les mesures de surveillance internationale concernées par le présent recours 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.

24 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.

25 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. Il n'y a donc aucune raison que cet article s'y applique. Pourtant, c'est bien sur lui que la charge de la preuve repose, les mesures en cause étant par définition secrète.

26 **Par conséquent,** la juridiction administrative compétente peut être saisie pour tout recours contre une décision concernant des mesures de surveillance internationale antérieures au 2 décembre 2015.

27 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, les dispositions de l'article L. 854-9 sont inapplicables et ne peuvent donc avoir pour effet d'évincer le droit de saisir une juridiction administrative d'un recours pour excès de pouvoir.

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

28 Au surplus, le Conseil d'État devra interpréter les dispositions nationales en vigueur à la lumière de la directive 2016/680.

29 **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.

30 La Directive impose notamment que « sans préjudice de tout autre recours administratif ou extrajudiciaire, les États membres prévoient qu'une personne 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).

31 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 être transposée (CJCE, 6e, 8 oct. 1987, *Kolpinghuis Nijmegen*, 80/86).

32 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).

33 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, 9e et 10e SSR, 10 janv. 2001, *France Nature Environnement*, no 217237)

34 **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

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

35 À titre liminaire, il convient de rappeler que la protection des droits reconnus par la Charte doit trouver son plein effet en l'occurrence. [3]

36 Le Premier ministre fait valoir que la législation française sur les mesures de surveillance internationale ne mettrait pas en œuvre le droit de l'Union et que, dès lors, la Charte n'est pas invocable dans le présent litige. Il avance au soutien de cette position deux arguments : d'une part, cette législation relève de la défense et de la sûreté de l'État et, d'autre part, elle ne régirait pas l'activité des fournisseurs de services de communications électroniques.

37 **En droit,** des mesures nationales permettant aux autorités l'interception et/ou l'accès aux communications électroniques, ainsi qu'aux données 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)

38 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

3. Voir la section 3 page 7 du mémoire ampliatif du 13 novembre 2016.

celle-ci du respect de la Charte. [4]

39 **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.

40 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.

41 **Par conséquent,** les mesures de surveillance internationale en cause doivent être conformes au droit de l'Union et notamment à la directive 2002/58 interprétée à la lumière de la Charte.

42 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 18).

43 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

44 **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.

45 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 relève 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

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

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)

46 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).

47 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 soulignait 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 ÉtatsUnis, 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 ÉtatsUnis 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 ÉtatsUnis [...]. » (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 ÉtatsUnis 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 ÉtatsUnis » (cité au point 25).

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

49 **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 correspondent 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. ¶ 45 page 8).

50 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. [. . .] »

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

52 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. »

53 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.

54 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.

55 **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.

56 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

57 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).

58 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

59 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.

60 **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.

61 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).

62 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*).

63 **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.

64 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 ; »

65 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. »

66 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 »

67 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)

68 Ainsi, force est de constater que les finalités poursuivies au 5° et 6° de l'article L. 811-3 dépasse 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.

69 **En conséquence,** les objectifs poursuivis par les mesures de surveillance internationale mises en œuvre avant ne sont pas suffisamment limités.

70 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

71 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).

72 **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*).

73 **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.

74 **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.

75 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 prove-

> nance 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...

76 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.

77 **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 indépendante, et que **la 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)

78 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.

79 **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 agence 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 internationale [5].

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

5. 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

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 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. [6]

81 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

6. 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.

en France avaient été transmises par la DGSE à la NSA [7]. 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 français [8].

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

82 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 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.

83 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.

84 **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. »

85 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 violes, 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. »

7. 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.

8. 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.

86 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).

87 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).

88 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, 4e sect., 18 mai 2010, *Kennedy c. R-U*, n° 26839/05, § 124).

89 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.

90 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).

91 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.).

92 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).

93 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).

94 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)

95 **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 »

96 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 informent 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)

97 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.

98 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.

99 **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.

100 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.

101 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.

102 **Par conséquent,** en n'ayant pas informé 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.

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 dans son action contre les décisions d'autorisation, de mise en œuvre et/ou de contrôle des mesures de surveillance internationale initiées depuis 2008 et révélées par la presse. ;
— 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 cessation desdites mesures ainsi qu'à la destruction des renseignements concernant Madame In 't Veld.

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 20 mars à Paris,

Hugo ROY
AVOCAT AU BARREAU DE PARIS

TABLE DES JURISPRUDENCES