

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

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

OBSERVATIONS COMPLÉMENTAIRES

POUR : **1/ La Quadrature du Net**
2/ French Data Network
3/ La Fédération des fournisseurs d'accès à Internet associatifs

SCP SPINOSI & SUREAU

CONTRE : **Le Premier ministre.**

Sur la requête n° 394.924

DISCUSSION

I. En réponse au mémoire en défense en date du 21 avril 2015 déposé par le Premier ministre, les associations exposantes entendent verser aux débats les observations suivantes.

Persistant dans l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures, les exposantes entendent plus particulièrement réfuter l'argumentation présentée par le Premier ministre dans son mémoire, mais aussi faire valoir des moyens complémentaires tirés du droit de l'Union européenne.

II. D'emblée, pour la parfaite information du Conseil d'Etat, les associations tiennent cependant à souligner que le présent recours initié contre le décret n° 2015-1186 du 29 septembre 2015 présente des liens de connexité avec les recours initiés contre quatre autres décrets d'application de la loi relative au renseignement (enregistrés sous les n^{os} 394.922, 394-925 et 397.851 pour les recours des trois associations exposantes, ainsi que sous le n° 397.844 pour le recours de l'association Igwan.net, adhérente de la FFDN).

Sur l'intérêt à agir

III. En premier lieu, le Premier ministre prétend qu'« aucune des dispositions du décret ne porte atteinte aux intérêts que les associations requérantes se sont données pour objet de défendre » (cf. le mémoire en défense, page 1).

Or, il n'en est rien.

III-1 En effet, il convient de rappeler que les associations exposantes ont pour mission statutaire d'agir pour la défense des droits fondamentaux dans l'environnement numérique mais aussi – s'agissant plus particulièrement de la FDN et de la FFDN – de protéger les droits de ses adhérents et abonnés dans le cadre de l'accès à Internet.

Un tel constat n'est aucunement contesté par le Premier ministre, lequel ne nie pas davantage que les dispositions de la loi relative au renseignement sont de nature à affecter ces intérêts statutaires.

Tout au plus est-il affirmé que le décret contesté, en ce qu'il est relatif à l'organisation administrative et financière de la Commission nationale de contrôle des techniques de renseignement (ci-après CNCTR), n'affecterait pas ces intérêts.

III-2 Une telle assertion méconnaît toutefois radicalement le rôle central de la CNCTR dans le dispositif prévu par le législateur.

Il importe ainsi de rappeler que le Conseil constitutionnel a lui-même souligné que « *la commission nationale de contrôle des techniques de renseignement* » est chargée avec le Conseil d'Etat « *de s'assurer du respect de [l']exigence de proportionnalité* » qui s'impose en particulier à la « *décision de recourir aux techniques de renseignement et [aux] techniques choisies* » (Cons. constit. Décision n° 2015-713 DC du 23 juillet 2015, not. cons. 11).

De façon significative, concernant les techniques de surveillance des communications internationales, l'absence d'un tel « *contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre* » a d'ailleurs justifié, notamment, la censure par le Conseil constitutionnel des dispositions relatives à cette surveillance internationale (*Ibid.* cons. 78).

Partant, les conditions dans lesquelles fonctionne la CNCTR affectent directement la mise en œuvre mais aussi le contrôle des techniques de renseignement prévues par la loi du 24 juillet 2015.

Or, tel est précisément l'objet du décret attaqué.

Au demeurant, les premiers mois d'existence de la CNCTR ont amplement confirmé que ses difficultés matérielles et organisationnelles sont susceptibles d'en altérer fortement le bon fonctionnement (v. Marc Rees, « Loi Renseignement : le cri d'alarme du surveillant des surveillants », *in NextInpact*, 16 février 2016 - **Prod. 1**).

Dès lors, le décret est bien susceptible de porter atteinte aux intérêts statutaires des associations exposantes, lesquelles peuvent valablement le contester notamment en ce qu'il permet la mise en œuvre d'un dispositif légal qui, lui-même, affecte directement ces intérêts.

Sur la méconnaissance de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

IV. En deuxième lieu, le Premier ministre tente de faire valoir que les moyens tirés du défaut de base légale du décret litigieux en raison de l'inconventionnalité des dispositions de la loi relative au renseignement serait « *irrecevables* » et « *en tout état de cause infondées* » (cf. le mémoire en défense, page 2).

Mais aucun des arguments du Premier ministre ne saurait convaincre.

V. S'agissant d'abord de la recevabilité, il importe de rappeler que le décret litigieux est indissociable de l'ensemble du dispositif ainsi créé par la loi relative au renseignement, tant l'existence même de la CNCTR et son bon fonctionnement conditionne la constitutionnalité des techniques de renseignement prévues par un tel dispositif (cf. *supra* au point **III-2** et au point **VII** du mémoire complémentaire).

Il est donc manifeste que ce décret a bien été pris en application des dispositions du Livre VIII du code de la sécurité intérieure (Partie législative), lesquelles sont elles-mêmes inséparables et forment un tout en particulier s'agissant des mécanismes de contrôle dont la conventionnalité est précisément ici en cause.

Les moyens tirés de l'inconventionnalité des dispositions légales ne sont donc aucunement irrecevables.

VI. Pour ce qui est ensuite de leur bien-fondé, compte tenu de l'argumentation du Premier ministre, les associations exposantes ne peuvent que persister à souligner combien les dispositions du livre VIII du code de la sécurité intérieure ainsi que les articles L. 773-1 à

L. 773-8 du code de justice administrative méconnaissent le droit au respect de la vie privée et le droit au recours effectif garantis par les articles 8 et 13 de la Convention européenne

Et ce, toujours à deux titres.

VI-1 D'une part, la seule circonstance que la Cour européenne ait admis qu'à défaut d'un dispositif de notification *a posteriori* des mesures de surveillance secrète, l'atteinte portée par ces mesures aux droits conventionnels peut potentiellement être compensée par un mécanisme effectif de contrôle en cas de soupçon de surveillance, ne saurait suffire en soi à justifier l'absence totale et par principe de tout dispositif de notification.

En effet, ainsi que les associations l'ont déjà souligné et conformément au principe de proportionnalité qui irrigue l'ensemble de l'analyse européenne, la Cour de Strasbourg admet certes l'existence d'impératifs pouvant justifier – par exception – l'absence de notification *a posteriori* systématique.

Néanmoins, la jurisprudence européenne insiste, par principe, sur l'importance du mécanisme de notification *a posteriori* en soulignant qu'« il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction » (Cour EDH, G.C. 4 décembre 2015, *Roman Zakharov c. Russie*, Req. n° 47143/06, § 287).

Pour appuyer une telle assertion, la Grande Chambre de la Cour européenne a d'ailleurs indiqué « *prend[re] acte de la recommandation du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, laquelle dispose que lorsque des données concernant une personne ont été collectées et enregistrées à son insu, elle **doit**, si les données ne sont pas détruites, être informée, si cela est possible, que des informations sont détenues sur son compte, et ce dès que l'objet des activités de police ne risque plus d'en pâtir (point 2.2, paragraphe 143 ci-dessus).* » (*Ibid.*).

En somme, si l'obligation de notification est certes conditionnée à plusieurs circonstances, lesquelles peuvent justifier qu'il y soit dérogé par exception, il n'en demeure pas moins que cette obligation doit par principe être respectée autant que possible.

En particulier, lorsque la notification *a posteriori* n'est aucunement susceptible « *de compromettre le but à long terme qui motivait à l'origine la surveillance* » (*Roman Zakharov c. Russie*, précité, § 287), elle devrait être prévue et mise en œuvre de façon individualisée aux fins de garantir une protection optimale des droits et libertés conventionnels.

Or, en ne prévoyant strictement aucun dispositif – fut-il conditionné – de notification *a posteriori*, les dispositions légales contestées ont radicalement méconnu les exigences tirées des articles 8 et 13 de la Convention.

En tout état de cause, une telle conclusion s'impose nécessairement faute de mécanismes compensatoires effectifs et suffisants.

VI-2 D'autre part, en effet, à rebours des assertions du Premier ministre, il apparaît que le dispositif prévu par la loi relative au renseignement n'est aucunement « *assorti, à tous les stades de la surveillance, de modalités de contrôle constituant des garanties suffisantes* ».

VI-2.1 Premièrement, il est particulièrement révélateur que le Premier ministre s'abstienne de répondre aux arguments des associations concernant le fait que la procédure de saisine de la CNCTR ou du Conseil d'Etat prévue aux articles L. 833-4 et L. 841-1 du code de la sécurité intérieure ne permet aucunement à la personne qui soupçonne qu'une technique de renseignement a été mise en œuvre à son égard d'obtenir ne serait-ce que la confirmation ou l'infirmerie d'une telle surveillance (cf. le mémoire complémentaire au point **X-2**).

Ce seul constat suffit donc à confirmer la méconnaissance des exigences conventionnelles selon lesquelles l'intéressé doit disposer d'une « possibilité satisfaisante de demander et d'obtenir auprès des

autorités des informations sur les interceptions », mais d'un « droit d'accès aux documents relatifs à l'interception de ses communications » (*Roman Zakharov c. Russie*, précité, § 298 et 290).

Sans doute dans l'espoir de compenser cette carence manifeste, tout au plus le Premier ministre tâche-t-il de faire valoir que la CNCTR, par contraste, « *dispos[e] d'un plein accès aux éléments classifiés de la procédure* » (cf. le mémoire en défense, page 3).

Mais une telle circonstance ne saurait en aucune façon pallier la méconnaissance du droit propre à l'intéressé de disposer lui-même des informations, d'autant que la CNCTR n'a pas pour mission légale de représenter et d'assurer la défense des personnes faisant l'objet d'une surveillance, ni même de protéger spécifiquement leurs droits.

En outre, et en tout état de cause, les dispositions légales contestées ne mettent pas la CNCTR en mesure d'exercer un contrôle effectif et suffisant.

VI-2.2 Deuxièmement, en effet, il convient de rappeler que si l'« *autorisation préalable du Premier ministre* » prévue à l'article L. 821-1 du code de la sécurité intérieure pour la mise en œuvre de techniques de surveillance n'est en principe certes « *délivrée [qu']après avis de la Commission nationale de contrôle des techniques de renseignement* », le Premier ministre peut se passer d'un tel avis préalable « *en cas d'urgence absolue* », au sens de l'article L. 821-5 du même code.

Or, pour faire valoir que de tels cas seraient « *strictement encadrés par la loi* », le Premier ministre fait valoir que la CNCTR « *est informée sans délai* » et qu'elle peut « *s'assurer que le cadre légal a été respecté* » (cf. le mémoire en défense, page 3).

Mais il n'en est rien.

En effet, la CNCTR ne dispose d'aucun pouvoir de contrainte ou d'injonction envers l'autorité administrative, puisqu'elle ne peut que formuler de simples avis ou recommandations qui ne lient pas le Premier ministre.

Dès lors, le droit d'accès et d'information qui est reconnu à la CNCTR et dont se prévaut le Premier ministre ne saurait constituer une garantie effective au sens des exigences européennes.

Tout au plus la CNCTR peut-elle saisir le Conseil d'Etat en vertu de l'article L. 833-8 du code de la sécurité intérieure.

Mais **non seulement** cette saisine n'est qu'une simple possibilité, et non une obligation prévue par les dispositions légales contestées.

A cet égard, il n'est pas inutile de relever que cette carence législative – cumulée aux moyens matériels limités de la CNCTR (cf. **Prod. 1**) – a conduit son actuel Président à indiquer dès avant son entrée en fonction qu'il n'entendait pas saisir systématiquement le Conseil d'Etat en cas de non respect par le Premier ministre des avis de la CNCTR – aux motifs, selon lui, que « *l'épicentre du contrôle ne doit pas basculer du côté juridictionnel* » (Audition de Francis Delon devant la Commission des lois du Sénat, 29 septembre 2015).

En outre, cette éventuelle saisine du Conseil d'Etat ne permettrait toujours pas à la personne concernée par la surveillance potentielle de prendre elle-même connaissance des informations la concernant.

Enfin, il y a lieu de souligner que la Cour européenne ne requiert pas tant l'intervention d'une autorité administrative indépendante que l'existence de voies de recours effectives (*Roman Zakharov c. Russie*, précité, § 234 et 286 et s.).

Or, en l'occurrence, il n'en est rien.

Et ce, pour de nombreuses raisons dont les trois suivantes qui seront développées plus avant concernant notamment la contrariété des dispositions légales contestées au regard du droit de l'Union européenne :

- L'administration contrôle pleinement l'accès du requérant aux informations classifiées, ce qui porte manifestement atteinte principes du procès équitable (cf. *infra* au point **XXIV-3**);
- Aucun dispositif n'a été prévu pour permettre au requérant d'avoir accès aux informations classifiées (cf. *infra* au

point **XXIV-4**) ;

- Le recueil et l'exploitation par les services français de renseignements transmis par des services étrangers ne peuvent faire l'objet d'aucun recours juridictionnel (cf. *infra* au point **XXIV-2**).

VIII. Partant, la méconnaissance des exigences conventionnelles par les dispositions de la loi relative au renseignement est manifeste, de sorte que la censure du décret litigieux pris sur ce fondement est certaine.

Une telle conclusion s'impose d'autant plus eu égard aux autres moyens que les associations entendent soulever.

Sur la méconnaissance de la Charte des droits fondamentaux de l'Union européenne par la loi relative au renseignement

IX. En troisième lieu, les dispositions du décret contesté sont illégales en l'absence de toute base juridique qui en permettent l'édiction, compte tenu de la contrariété des dispositions législatives que les dispositions réglementaires mettent en œuvre avec la Charte des droits fondamentaux de l'Union européenne.

Et ce, à plusieurs égards.

X. D'emblée, il y a lieu de rappeler que les dispositions du décret contesté mettent en œuvre l'ensemble du dispositif légal prévu au Livre VIII du code de la sécurité intérieure, tel que créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement (cf. le mémoire complémentaire au point **VII**).

XI. En outre, et **à titre liminaire**, il convient de souligner que la Charte des droits fondamentaux est bien invocable en l'occurrence.

En effet, tant le décret contesté que la loi relative au renseignement « *mettent en œuvre le droit de l'Union* » au sens exact des stipulations

de l'article 51, al. 1^{er}, de la Charte et de la jurisprudence de la Cour de justice de l'Union européenne.

XI-1 En ce sens, et d'une part, il y a lieu de relever que les dispositions réglementaires et législatives contestées concernent notamment le traitement des données à caractère personnel et affectent la protection de la vie privée dans le secteur des communications électroniques.

Or, ces domaines et enjeux font incontestablement partie du champ matériel du droit de l'Union européenne, qu'il s'agisse des articles 7 et 8 de la Charte – relatifs respectivement au droit au respect de la vie privée et familiale et au droit à la protection des données personnelles – ou encore de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

En outre, le fait que les dispositions réglementaires et législatives contestées relèvent de matières régies par le droit de l'Union implique que celles-ci respectent les droits fondamentaux reconnus par la Charte, ainsi qu'il résulte de la jurisprudence de la Cour de justice de l'Union européenne selon laquelle *« les droits fondamentaux garantis par la Charte devant, par conséquent, être respectés lorsqu'une réglementation nationale entre dans le champ d'application du droit de l'Union, il ne saurait exister de cas de figure qui relèvent ainsi du droit de l'Union sans que lesdits droits fondamentaux trouvent à s'appliquer. L'applicabilité du droit de l'Union implique celle des droits fondamentaux garantis par la Charte. »* (CJUE, G.C., 26 fév. 2013, Åklagaren, C-617/10, § 21).

XI-1.1 En particulier, l'objet de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 (directive dite « ePrivacy ») vise *« à garantir le plein respect des droits exposés aux articles 7 et 8 »* de la Charte des droits fondamentaux (considérant 2).

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

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

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

XI-1.2 Plus spécifiquement encore, l'article 15 de la directive précitée mentionne explicitement les droits et obligations en matière de confidentialité des communications et d'anonymisation des données définis par les articles 5, 6, 8, paragraphes 1, 2, 3 et 4, et par l'article 9 de la directive 2002/58.

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

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

« 1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent

à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. [...] »

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

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

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

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

XI-1.3 Or, en l'espèce, il ne fait aucun doute que les mesures et techniques autorisées par les dispositions légales litigieuses constituent bien une limitation des droits et obligations précités et devront, comme l'exigent les stipulations de la Charte, être nécessaires, appropriées et proportionnées dans une société démocratique.

En effet, parmi les techniques de renseignement prévues au titre V du Livre VIII du code de la sécurité intérieure – tel qu'issu de la loi relative au renseignement – figure notamment à l'article L. 851-1 le recueil par l'administration, auprès des opérateurs de communications électroniques et des hébergeurs, des « *données techniques [...] de connexion à des services de communications électroniques* », des données relatives « *à la localisation des équipements terminaux utilisés* » et, plus généralement le recueil des données conservées en application de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ainsi que du II de l'article 6 de la loi n° 2004-575 dite LCEN (Sur le dispositif similaire en vigueur antérieurement, v. Cons. const., juillet 2015, décision QPC n° 2015-478, cons. 12).

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

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

XI-2 D'autre part, il n'est pas inutile de souligner que la seule circonstance que les dispositions réglementaires et législatives contestés soient – notamment – motivées par la sauvegarde de la sécurité nationale ne saurait avoir pour conséquence de les soustraire au respect du droit de l'Union européenne, dès lors que ces mesures constituent une limitation des droits et obligations résultant de la mise en œuvre du droit de l'Union.

De fait, il est indéniable que les mesures poursuivant un objectif de sauvegarde de la sécurité nationale sont explicitement visées par la directive 2002/58/CE.

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

Au contraire, de telles mesures s'inscrivent dans un ensemble juridique cohérent relatif à la conservation des données dans l'objectif de sauvegarder la sécurité nationale.

Un tel constat est amplement conforté par le récent règlement général sur la protection des données n° 2016/679 en date du 27 avril 2016, publié au Journal Officiel de l'Union européenne le 4 mai 2016 et qui remplacera la directive 95/46/CE le 25 mai 2018.

En effet, en son article 23, ce règlement dispose que si « *le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus* » par certaines de ses stipulations (transparence, droit à l'information et à l'accès aux données à caractère personnel, droits de rectification et d'effacement, droit d'opposition, etc.), une telle limitation est expressément conditionnée à la nécessité qu'elle :

« Respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir [notamment] :

- a) la sécurité nationale;*
- b) la défense nationale;*
- c) la sécurité publique;*

d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; [...] »

Partant, et là encore, il apparaît nettement que si des impératifs tenant à la protection de l'ordre public – dont la sécurité nationale – peuvent justifier des limitations aux droits et libertés garantis par le droit de l'Union, ils ne sauraient conduire à l'exclusion pure et simple de ces droits et libertés.

Au demeurant, raisonner différemment reviendrait à priver l'article 51.1 de la Charte des droits fondamentaux de tout effet utile, puisqu'il suffirait à chaque Etat membre de revendiquer la poursuite d'un objectif de sécurité nationale pour soustraire n'importe quelle mesure du contrôle conformité aux droits et libertés protégés par cette Charte.

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

XI-3 Enfin, il est utile de préciser que le fait que les dispositions législatives et réglementaires contestées résultent d'une exception ou d'une dérogation prévues par le droit de l'Union ne saurait les soustraire à l'impératif de respecter les droits fondamentaux garantis par la Charte, et ce, y compris lorsqu'elles sont motivées par des raisons impérieuses d'intérêt général.

A cet égard, la jurisprudence de la Cour de justice de l'Union européenne est sans aucune ambiguïté.

En effet, *« lorsqu'il s'avère qu'une réglementation nationale est de nature à entraver l'exercice de l'une ou de plusieurs libertés fondamentales garanties par le traité, elle ne peut bénéficier des exceptions prévues par le droit de l'Union pour justifier cette entrave que dans la mesure où cela est conforme aux droits fondamentaux dont la Cour assure le respect. Cette obligation de conformité aux*

*droits fondamentaux relève à l'évidence du champ d'application du droit de l'Union et, en conséquence, de celui de la Charte. L'emploi, par un État membre, d'exceptions prévues par le droit de l'Union pour justifier une entrave à une liberté fondamentale garantie par le traité doit, dès lors, être considéré, ainsi que Mme l'avocat général l'a relevé au point 46 de ses conclusions, comme «mettant en œuvre le droit de l'Union», au sens de l'article 51, paragraphe 1, de la Charte » (CJUE, 3^e ch., 30 avr. 2014, *Pfleger et a.*, C-390/12, point 36 ; voir également en ce sens, l'arrêt *ERT*, 18 juin 1991, C-260/89, point 43).*

Dès lors, le fait que les dispositions en cause procèdent d'une marge de liberté accordée aux États membres par l'article 15 de la directive 2002/58 ne saurait être interprété comme créant un champ autonome du droit de l'Union. Au contraire, l'usage de cette liberté par un État membre doit être considéré comme une mise en œuvre du droit de l'Union dans laquelle le respect de la Charte s'impose.

XII. Or, tel est précisément le cas des dispositions législatives litigieuses – ainsi que des dispositions réglementaires qui les mettent en œuvre –, de sorte que les exigences de la Charte des droits fondamentaux de l'Union européenne leur sont indubitablement applicables.

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

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

« Une législation nationale – telle que la loi française relative au renseignement en date du 24 juillet 2015 ou celle relative aux mesures de surveillance des communications électroniques internationales du 30 novembre 2015 – qui a pour objet d'autoriser les services de renseignement à recourir à de multiples techniques de surveillance, tel le recueil de données de connexion, relève-t-elle des « mesures législatives visant à limiter la portée des droits et des obligations » au sens de l'article 15.1 de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ; et, corrélativement mais aussi au regard de l'objet même de cette législation, met-elle « en œuvre le droit de l'Union » au sens des stipulations de l'article 51, al. 1^{er}, de la Charte des droits fondamentaux de l'Union européenne de sorte que les droits et libertés prévus notamment par les articles 7 et 8 de cette Charte lui sont opposables ?

Corrélativement, l'arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12) doit-il être interprété en ce sens qu'il pose des exigences, au regard des articles 7 et 8 de la Charte, qui s'imposent à un régime national régissant la conservation des données relatives à des communications électroniques et l'accès à de telles données ? »

XIII. Par ailleurs, et **toujours à titre liminaire**, les associations entendent préciser qu'il y a lieu d'interpréter les droits et libertés garantis par la Charte des droits fondamentaux à l'aune des exigences de la Convention européenne des droits de l'homme et des libertés fondamentales ainsi que de la jurisprudence de la Cour européenne des droits de l'homme.

En effet, aux termes des stipulations de l'alinéa 3 de l'article 52 de la Charte, *« dans la mesure de la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».*

Or, il en est ainsi, et notamment, pour le droit au respect de la vie privée et familiale et du droit à la protection des données personnelles

ou encore pour le droit à un recours effectif et à accéder à un tribunal impartial, chacun étant garanti tant par la Charte que par la Convention européenne.

En ce qui concerne la méconnaissance du droit au respect de la vie privée et du droit à la protection des données personnelles

XIV. Premièrement, les dispositions du livre VIII du code de la sécurité intérieure intitulé « *Du renseignement* » ainsi que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, portent atteinte aux droits au respect de la vie privée et à la protection des données personnelles, en tant qu'elles portent une atteinte disproportionnée aux droits au respect de la vie privée et familiale ainsi qu'au droit à la protection des données personnelles.

Sur l'ampleur de l'ingérence

XIV-1 En droit, aux termes de l'article 7 de la Charte des droits fondamentaux, « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ».

En outre, selon l'article 8 de la Charte des droits fondamentaux :

« 1. *Toute personne a droit à la protection des données à caractère personnel la concernant.*

2. *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*

3. *Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »*

De plus, l'article 52 de la même Charte stipule que :

« 1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

2. Les droits reconnus par la présente Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci.

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue. »

XIV-2 Sur le fondement de ces stipulations, et toujours en droit, la Cour de justice de l'Union européenne considère que, « *pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence* » (CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12, § 33).

De plus, la Cour considère que « *l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental* » et « *qu'il existe un risque important d'accès illicite à ces données* » lorsque celles-ci « *sont soumises à un traitement automatique* » (*Ibid.* § 35 et 55).

Ensuite, la Cour de justice estime que « *la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (*Ibid.* § 37).

Enfin, elle considère que les « *données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile [...] sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* » (Ibid. § 37).

En somme, les techniques de recueil de renseignement qui permettent notamment l'accès, la conservation et l'exploitation de données de connexion sont éminemment intrusives en ce qu'elles permettent de révéler un volume considérable d'informations personnelles.

Car, pour reprendre les conclusions de l'avocat général VILLALON sur l'affaire *Digital Rights Ireland et Seitlinger e.a.*, « *les effets de cette ingérence se trouvent démultipliés par l'importance acquise par les moyens de communications électroniques dans les sociétés modernes, qu'il s'agisse des réseaux mobiles numériques ou d'Internet, et leur utilisation massive et intensive par une fraction très importante des citoyens européens dans tous les champs de leurs activités privées ou professionnelles. Les données en question, il importe également d'insister encore une fois à cet égard, ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée* » (Ibid., § 73-74).

Très récemment, pour décider de soumettre l'examen d'une question préjudicielle à la procédure accélérée, le Président de la Cour de justice de l'Union européenne a d'ailleurs réaffirmé fermement que « *qu'une réglementation nationale permettant la conservation de toutes les données relatives à des communications électroniques ainsi que l'accès ultérieur à ces données est susceptible de comporter des*

ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte (voir arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 37). » (Ordonnance du Président de la CJUE, 1er février 2016, Aff. C-698/15).

XIV-3 Or, en l'espèce, il convient de rappeler que le titre V du livre VIII du code de la sécurité intérieure prévoit huit techniques de recueil de renseignements.

Trois de ces techniques visent à collecter le contenu d'informations échangées ou détenues par des individus :

- L'interception de correspondances électroniques (Art. L. 852-1)
- La captation de paroles et d'images privées, notamment par intrusion dans un lieu privé et pose de caméra ou de micro (Art. L. 853-1);
- L'accès à un appareil informatique, à distance ou par intrusion dans un lieu privé (Art. L. 853-2) ;

Une de ces techniques concerne la collecte de toute information traitée par un opérateur de communications électroniques, un fournisseur d'accès à Internet ou un hébergeur, visant notamment les « *données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs* » (Art. L. 851-1).

Deux autres de ces techniques visent à identifier ou localiser des individus :

- La collecte par un dispositif technique de données permettant l'identification ou la localisation d'appareils ou de leur utilisateur (Art. L. 851-6) ;
- La localisation en temps réel d'une personne ou d'une chose par pose d'un dispositif technique ou par recueil en temps réel auprès des opérateurs des données de localisation d'un appareil (Art. L. 851-4 et L. 851-5).

Deux dernières techniques sont spécifiques à la lutte contre le terrorisme et seront traitées ultérieurement dans des développements dédiés.

Toute ces techniques visent à collecter des informations qui relèvent tant de la vie privée que des données à caractère personnel. Ces informations sont recueillies et conservées dans des systèmes automatisés, afin que l'administration puisse y accéder, et sans que les personnes concernées n'en soient jamais informées.

Par conséquent, les dispositions législatives contestées autorisent des techniques de surveillance qui constituent pour chacune une ingérence dans et une limite aux droits garantis aux article 7 et 8 de la Charte.

De plus, au regard de la jurisprudence de la Cour de justice, elles sont d'une particulière gravité, chacune de ces ingérences présentant un « *risque important d'accès illicite* » par l'administration et étant « *susceptible de générer dans l'esprit des personnes [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 37).

XIV-4 C'est donc à l'aune de l'importante gravité des ingérences litigieuses qu'il convient d'apprécier l'existence de garanties légales suffisantes pour en assurer la proportionnalité, ainsi que l'exigent les stipulations de l'article 52, paragraphe 1, de la Charte.

Or, en l'occurrence, l'insuffisance de ces garanties est manifeste.

Et ce, à plusieurs égards.

Sur l'insuffisante précision des finalités susceptibles de justifier l'ingérence

XV. D'une part, les dispositions légales contestées ne satisfont pas à l'exigence de stricte précision des finalités susceptibles de justifier l'ingérence.

XV-1 En effet, en droit, en application de l'article 52, al. 1^{er}, de la Charte, la Cour de justice de l'Union considère qu'est contraire à la Charte toute mesure de surveillance qui « *ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence* » (CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12, § 60) ou, plus précisément, une mesure poursuivant autre chose que « *des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* » (CJUE, 6 octobre 2015, *Schrems*, C-362/14, § 93).

Ce faisant, la Cour de justice reprend l'analyse de la Cour européenne des droits de l'homme selon laquelle « *le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (Cour EDH, Pl. 6 septembre 1978, *Klass et autres c. Allemagne*, Req. n° 5029/71, § 42). Plus précisément encore, la Cour de Strasbourg souligne que « *la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète* », car la loi « *irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites* » (Cour EDH, 2 août 1984, *Malone c. Royaume-Uni*, Req. n° 8691/79 ; v. aussi Cour EDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, Req. n° 54934/00, § 95).

XV-2 Or, en l'occurrence, les dispositions de l'article L. 811-3 du code de la sécurité intérieure prévoient que de nombreux services de l'administration peuvent mettre en œuvre les mesures de surveillance définies plus tôt pour recueillir tout renseignement susceptible de permettre la défense ou la promotion d'intérêts d'une grande diversité.

Cinq de ceux-ci sont particulièrement larges.

XV-2.1 D'abord, il en va ainsi des « *intérêts majeurs de la politique étrangère* » de la France visés au 2° de l'article L. 811-3, dont la loi ne limite aucunement la portée et en laissent donc l'entière délimitation au pouvoir exécutif, lequel détermine la politique étrangère de la France.

Ainsi, la loi ne limitant pas ces intérêts à la seule protection de la population, ceux-ci peuvent couvrir la mise en œuvre de stratégies politiques de nature et d'importance variables – dès lors susceptibles de concerner un large part de la population – et que le pouvoir exécutif arrête librement.

La défense ou la promotion de ces intérêts ne sont ainsi manifestement pas des finalités « *précises, strictement restreintes et susceptibles de justifier [la grave] ingérence* » qu'elles permettent.

XV-2.2 Ensuite, il en va de même de « *l'exécution des engagements européens et internationaux de la France* », visée au même 2° de l'article L. 811-3, qui couvre des engagements particulièrement variés et nombreux.

Ainsi, par exemple, au titre de cette finalité, l'administration est autorisée à intercepter toute communication susceptible de révéler des renseignements facilitant la mise en œuvre par la France des traités concernant les changements climatiques (Convention de New-York de 1992), la biodiversité (Convention de Rio de 1992), le droit d'auteur (Convention universelle du 24 juillet 1971) ou le droit de timbre en matière de chèques (Convention de Genève de 1931).

Il en va de même pour toutes les obligations auxquelles la France est soumise en application de l'ensemble du droit de l'Union européenne, couvrant des domaines aussi divers que l'agriculture, la pêche, les transports, l'emploi, la culture, la santé ou le tourisme.

Enfin, la loi ne vise pas exclusivement les engagements actuellement en vigueur mais couvrira tout engagement futur, dont la portée et le nombre sont par essence indéfinis.

Dès lors, en visant des engagements couvrant des domaines aussi larges ou non encore définis, la loi a manqué de limiter les ingérences

qu'elle permet aux seules finalités précises, restreintes et susceptibles de les justifier.

XV-2.3 En outre, le caractère excessif de la marge de manœuvre laissée à l'administration pour surveiller la population est le plus manifeste s'agissant de la défense des « *intérêts économiques, industriels et scientifiques majeurs de la France* », visée au 3° de l'article L. 811-3.

En effet, nul ne saurait raisonnablement prétendre pouvoir définir les contours concrets de tels intérêts, lesquels conditionnent pourtant une surveillance ainsi définie unilatéralement par le pouvoir exécutif sans prévisibilité pour la population susceptible d'en être affectée.

XV-2.4 De plus, il importe de relever que la prévention des « *violences collectives de nature à porter gravement atteinte à la paix publique* », visée au 5°, c, de l'article L. 811-3, a été regardée par le Conseil constitutionnel comme renvoyant à la prévention des infractions définies aux articles 431-1 à 431-10 du code pénal (Conseil constit., 23 juillet 2015, DC n°2015-713, cons. 10).

Dès lors, l'administration est habilitée à recourir à des techniques de renseignement susceptibles de fournir des informations concernant l'organisation d'une « *manifestation sur la voie publique n'ayant pas fait l'objet d'une déclaration préalable* » ou ayant fait l'objet d'une « *déclaration incomplète* » - infraction définie à l'article 431-9 du code pénal -, sans même avoir à démontrer le caractère violent de cette manifestation ni son caractère de nature à porter atteinte à la paix publique.

XV-2.5 Enfin, il n'en est pas différemment de la « *prévention de la criminalité et de la délinquance organisées* », visée au 6° de l'article L. 811-3 et que le Conseil constitutionnel, dans sa décision du 23 juillet 2015, a cette fois lié à la volumineuse liste des infractions visées à l'article 706-73 du code de procédure pénale.

Au titre de ces infractions se trouve celle définie à l'article 222-37 du code pénal qui punit « *l'acquisition ou l'emploi illicites de*

stupéfiants ». Or, la seule existence de soupçons quant à la commission d'une telle infraction – susceptible de concerner plusieurs millions d'adultes français, selon l'Observatoire français des drogues et des toxicomanies (cf. Beck F., Richard J.-B., Guignard R., Le Nézet O. et Spilka S., *Les niveaux d'usage des drogues en France en 2014*, exploitation des données du Baromètre santé 2014) – peut difficilement justifier qu'il soit porté une atteinte aussi importante à la vie privée.

Au demeurant, et plus largement encore, le libellé de l'article L. 811-3 du code de la sécurité intérieure n'autorise pas seulement la surveillance des personnes susceptibles de présenter un danger pour les intérêts qu'il vise, mais permet également le recours à des techniques de renseignement à toute personne susceptible de révéler des renseignements utiles à la défense de ces intérêts, peu importe d'ailleurs que ces personnes aient même conscience de pouvoir les révéler.

XV-3 Partant, il est manifeste que les dispositions de l'article L. 811-3 du code de la sécurité intérieure ne limitent pas les atteintes aux droits garantis aux articles 7 et 8 de la Charte aux seules « *finalités précises, strictement restreintes et susceptibles de justifier l'ingérence* », au sens de l'article 52 de cette même Charte et sont donc contraires à ces stipulations.

Une telle conclusion s'impose nécessairement, mais si le Conseil d'Etat avait un doute quant à la contrariété de cette disposition à la Charte, il aurait vocation à soumettre à la Cour de justice une question préjudicielle ainsi libellée :

« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant à un État membre de prévoir de façon secrète l'interception de communications privées, la pose de microphones ou de caméras dans des lieux d'habitation ou encore l'usage d'autres dispositifs intrusifs de surveillance dans le but de collecter tout renseignement susceptible de défendre ou de promouvoir des intérêts aussi vastes que : - les intérêts majeurs de sa politique étrangère ; - l'exécution de ses engagements européens et internationaux ; - ses intérêts économiques, industriels et scientifiques majeurs ; - la

prévention de l'organisation de manifestation non déclarée ou ayant fait l'objet d'une déclaration incomplète ; ou encore - la prévention de l'acquisition ou de l'emploi de stupéfiants à fins de consommation personnelle ? »

Sur la disproportion de l'ingérence née des techniques de renseignement prévues par le Titre V du Livre VIII du code de la sécurité intérieure

XVI. D'autre part, en prévoyant des techniques de renseignement excessivement intrusives, les dispositions contestées du Titre V du Livre VIII du code de la sécurité intérieure emportent une atteinte radicalement disproportionnée au regard des droits garantis par les articles 7 et 8 de la Charte.

Sur les dispositifs d'inspection du trafic prévu à l'article L. 851-3 du code de la sécurité intérieure (ou « boîtes noires »)

XVII. D'abord, les conditions dans lesquelles les dispositions de l'article L. 851-3 du code de la sécurité intérieure prévoient qu'« *il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* » constituent une ingérence disproportionnée compte tenu de la surveillance indiscriminée qu'elles impliquent.

XVII-1 En effet, et en droit, il convient de rappeler que par son récent arrêt *Digital Rights Ireland*, la Cour de justice de l'Union européenne a déclaré contraire aux articles 7 et 8 de la Charte la collecte de données de connexion concernant l'ensemble des utilisateurs de réseaux d'opérateurs, même ceux pour lesquels « *il n'existe **aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves*** », au lieu de se limiter aux seules « *personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales* » (CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12, § 58).

Plus récemment encore, de telles exigences ont également été affirmées solennellement par la Cour européenne des droits de l'homme. Dans son arrêt *Zakharov c. Russie*, la Grande Chambre a exigé que l'autorité à l'origine de l'ingérence soit « à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète » (Cour. EDH, Gr. Ch., 4 décembre 2015, *Zakharov c. Russie*, Req. n°47143/06)

Par ailleurs, il n'est pas inutile de préciser que, selon la Cour de justice, le caractère disproportionné de l'ingérence ainsi caractérisée ne dépend nullement du fait que les renseignements collectés sont ultérieurement exploités, car « *pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu [...] que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence* » (*Digital Rights Ireland*, précité, § 33). En particulier, le simple fait que des renseignements puissent être collectés « *sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (*Ibid.* § 37 ; en ce sens, v. Cour EDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, Req. n° 30562/04 et 30566/04, § 67).

XVII-2 Or, en l'occurrence, les dispositions de l'article L. 851-3, I, du code de la sécurité intérieure autorisent la mise en œuvre sur les réseaux d'opérateurs de « *traitements automatisés* » qui recueillent des informations ou documents concernant l'ensemble des communications transmises sur les réseaux ou serveurs concernés, afin de « *détecter des données susceptibles de caractériser l'existence d'une menace à caractère terroriste* ».

De la sorte, au moment du recueil de ces données, il n'existe strictement aucun « lien, même indirect ou lointain » entre les personnes concernées et l'existence d'une menace terroriste (cf. *Digital Rights Ireland*, précité, § 58), puisque le but de ces traitements est précisément d'établir un tel lien, afin que les services puissent ensuite surveiller les personnes identifiées de façon plus ciblée et s'assurer de

leur lien effectif avec une menace terroriste.

De plus, bien que l'article L. 851-3 prévoit, à son paragraphe I, que, dans un premier temps, ce traitement est réalisé « *sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent* », le paragraphe IV du même article prévoit que, dans un second temps, le Premier ministre peut autoriser « *l'identification de la ou des personnes concernées* » lorsqu'un possible lien avec une menace a été détecté.

Or, une telle identification est rendue possible par le fait que, parmi les données de connexion collectées par ces dispositifs, certaines sont des données personnelles, à l'image des adresses IP.

XVII-3 Dès lors, puisque les dispositions de l'article L. 851-3 du code de la sécurité intérieure autorisent la conservation de données identifiantes liées à des données techniques – susceptibles de révéler des parts importantes de la vie privée des personnes concernées – au sujet de nombreuses personnes qui ne présentent pourtant aucun « *lien, même indirect ou lointain, avec des infractions graves* », comme l'exige la Cour de justice de l'Union européenne, ces dispositions sont vouées à être déclarées contraires aux articles 7, 8 et 52 de la Charte.

Là encore, si le Conseil d'Etat devait avoir un doute quant à la conformité de cette disposition à la Charte, il devrait nécessairement soumettre à la Cour de justice une question préjudicielle demandant en substance ce qui suit :

« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant un État membre à collecter de façon indiscriminée et secrète des données techniques concernant l'ensemble des utilisateurs d'un réseau et pouvant être rattachées à ceux-ci ? »

Sur l'absence de limites à l'accès aux renseignements obtenus par la mise en œuvre d'une technique de renseignement

XVIII. Ensuite, l'absence d'encadrement légal des conditions d'accès

aux renseignements collectés en application des techniques prévues par le titre V constitue également une ingérence disproportionnée.

XVIII-1 En effet, et en droit, il y a lieu de souligner que dans son arrêt *Digital Rights Ireland*, la Cour de justice a explicitement souligné que « *n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données* [voir en ce sens, en ce qui concerne la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54), arrêt *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU:C:2014:238, points 57 à 61] » (*Digital Rights Ireland*, précité, § 93).

XVIII-2 Or, en l'occurrence, en dépit de leur importance et sensibilité, les renseignements collectés *via* les techniques prévues au Livre V précité sont potentiellement accessibles à quiconque sans aucun critère objectif délimitant cet accès comme l'exige pourtant le droit de l'Union européenne.

En effet, les dispositions des articles L. 811-1 et s. du code de la sécurité intérieure ne concernent que l'autorisation à utiliser les techniques de renseignement et non l'accès aux renseignements qui ont été collectés dans ce cadre.

Ainsi, les dispositions des deux derniers alinéas de l'article L. 822-1 se bornent à confier au Premier ministre la mission d'organiser « *la traçabilité de l'exécution des techniques autorisées en application du chapitre Ier du présent titre et définit les modalités de la centralisation*

des renseignements collectés » et indiquent qu' « à cet effet, un relevé de chaque mise en œuvre d'une technique de recueil de renseignement est établi. Il mentionne les dates de début et de fin de cette mise en œuvre ainsi que la nature des renseignements collectés. Ce relevé est tenu à la disposition de la commission, qui peut y accéder de manière permanente, complète et directe, quel que soit son degré d'achèvement ».

Il y a ainsi lieu de relever qu'aux termes de l'article R. 823-1 du code de la sécurité intérieure, cette mission a été confiée au groupement interministériel de contrôle, lequel est chargé de « *concourir à la traçabilité de l'exécution des techniques de recueil de renseignement* ».

Mais en écho au mutisme des dispositions législatives contestées, ces dispositions réglementaires ne prévoient aucun encadrement quant à la traçabilité des informations obtenues à l'issue de l'exécution des techniques : une fois la centralisation des données évoquée – dont les modalités réelles ne sont d'ailleurs pas précisées – rien n'est prévu pour encadrer l'accès aux données collectées.

Tout au plus l'article L. 822-3 du code de la sécurité intérieure énonce-t-il que « *les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3. Ces opérations sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement* » et que « *les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités* ».

Mais si ces dispositions tendent donc à préciser quelques-unes des conditions de collecte, transcription et extraction des renseignements obtenus, il n'en est strictement rien concernant leurs conditions d'accès ou de consultation par les autorités publiques.

XVIII-3 Partant, il est manifeste que les dispositions de l'article L. 822-3 du code de la sécurité intérieure ainsi que l'ensemble du dispositif institué par les articles L. 811-1 et suivant du même code méconnaissent les articles 7, 8 et 52 de la Charte, tels qu'interprétés de façon univoque par la Cour de justice.

Toute autre interprétation implique nécessairement que le Conseil d'Etat transmette à la Cour de justice de l'Union européenne la question préjudicielle suivante :

« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant un État membre à collecter, conserver et exploiter un ensemble de données sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques à ces données ? »

Sur le caractère excessif et disproportionné des durées de conservation des données

XIX. De troisième part, en vertu des dispositions de l'article L. 822-2 du code de la sécurité intérieure, les données collectées au titre des techniques de renseignement prévues par le Titre V du Livre VIII du code de la sécurité intérieure peuvent être conservées pendant des durées excessives, au surplus sans encadrement suffisant des finalités de telles conservations.

XIX-1 En droit, il importe de rappeler que dans son arrêt *Schrems* du 6 octobre 2015, la Cour de justice a estimé que « *n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes* » sans « *que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* » (CJUE, 6 octobre 2015, *Maximilian Schrems*, C-362/14, § 93). Etant précisé que la réalisation de cette dernière condition ne saurait en soi justifier le recours à un mécanisme de conservation généralisée des données.

Dans ce même arrêt, la CJUE considère aussi que « *la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire* » (*Ibid.* § 92).

À ce titre, la CJUE considère que « *la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire* », de sorte que n'est pas limitée au strict nécessaire « *une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues [...] en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées* » (CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12, § 63 et 64).

Cette jurisprudence doit s'analyser à la lumière de la jurisprudence de la Cour européenne des droits de l'homme d'après laquelle « *le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence [...] peu importe que les informations mémorisées soient ou non utilisées par la suite* » (Cour EDH, 4 décembre 2008, *Marper c. Royaume-Uni*, Req. n° 30562/04 et 30566/04, § 67).

XIX-2 Or, en l'occurrence, il convient de souligner que les dispositions de l'article L. 822-2 du code de la sécurité intérieure prévoient que les renseignements collectés au titre des techniques de renseignement précédemment exposées sont détruits au terme de :

- Trente jours pour le contenu des correspondances et les paroles privées (*i.e.* « *les correspondances interceptées en application de l'article L. 852-1 et pour les paroles captées en application de l'article L. 853-1 ;* »).
- Cent vingt jours pour les renseignements obtenus par intrusion informatique et pour les images privées (*i.e.* « *les renseignements collectés par la mise en œuvre des techniques mentionnées au chapitre III du titre V du présent livre, à l'exception des informations ou documents mentionnés à l'article L. 851-1* ») ;
- Quatre ans pour les données techniques (*i.e.* « *les informations ou documents mentionnés à l'article L. 851-1* ») ;

S'agissant spécifiquement « *des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement* » mais « *ils ne peuvent*

être conservés plus de six ans à compter de leur recueil ».

En outre, le 2° du III de l'article L. 851-6 du même code dispose que les informations ou documents recueillis sont « *détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre, dans un délai maximal de quatre-vingt-dix jours* ».

Sur la conservation des données de connexion

XIX-2.1 S'agissant **d'abord** de la conservation des données de connexion relatives aux communications électroniques ou à la contribution de contenu en ligne, il y a lieu de relever que les dispositions légales contestées distinguent le régime applicable à celles-ci du régime d'accès aux contenus des correspondances.

Or, en prévoyant une durée de conservation plus longue pour les métadonnées que pour les contenus, la loi procède à une différence qui n'est aucunement fondée « sur un critère objectif » au sens des exigences de la Cour de justice de (*Digital Rights Ireland*, précité, § 63 et 64).

En effet, il importe de rappeler que l'accès aux données de connexion ou métadonnées n'est pas, en soi, moins attentatoire aux droits et libertés garantis par les articles 7, 8 et 11 de la Charte ainsi que les articles 8 et 10 de la Convention européenne.

Comme l'ont relevé à raison M. Crepey, rapporteur public, dans ses conclusions présentées dans l'affaire n° 388134 (conclusions précédant la transmission de la question prioritaire de constitutionnalité dans l'affaire n° 2015-478 QPC), et M. Villalon, avocat général, dans ses conclusions précitées dans l'affaire *Digital Rights*, c'est à tort que l'ingérence dans la vie privée des personnes suscitée par l'accès aux métadonnées est souvent considérée comme moins grave que celle résultant de l'accès au contenu des correspondances. Et ce, compte tenu tant de l'évolution de la technologie et des usages, que de celle des techniques de collecte et d'analyse des renseignements recueillis.

Dans ces conditions, en portant à quatre ans la durée de conservation

des données de connexion, les dispositions légales ont porté une atteinte manifeste aux droits garantis par les articles 8 et 9 de la Charte des droits fondamentaux de l'Union européenne.

Sur la conservation des données chiffrées

XIX-2.2 Ensuite, il n'en est pas différemment pour la conservation de données chiffrées mentionnées au cinquième alinéa de l'article L. 822-2 du code de la sécurité intérieure.

D'emblée, il n'est pas inutile de préciser que ces renseignements chiffrés ne peuvent être des données de connexion. Dans la mesure où ces données sont des données relatives au trafic, elles sont toujours « *en clair* », puisqu'elles permettent l'acheminement du message chiffré.

En tout état de cause, un allongement de la durée de conservation des données à six ans lorsque celles-ci sont chiffrées n'est en aucun cas une mesure adaptée à la notion de données chiffrées.

En effet, l'expression « *données chiffrées* » peut recouvrir des réalités différentes. Le mode de chiffrement dépend du moment, dans la communication, où a lieu le chiffrement. D'une part, le chiffrement peut avoir lieu entre l'utilisateur et les prestataires de services de communications ; dans ce cas, chaque prestataire a accès au message en clair. D'autre part, le chiffrement peut être directement réalisé par l'émetteur pour ne pouvoir être lu que par son destinataire final, sans que les prestataires intermédiaires ne puissent y avoir accès en clair (chiffrement de « bout-en-bout »).

La méconnaissance des réalités techniques qui conduit à la suspicion associée aux informations et documents chiffrés est évidente dans le rapprochement fait au cinquième alinéa du I de l'article L. 822 du CSI entre les « documents et informations » issus des cyberattaques et les données chiffrées ou ayant été déchiffrées. Cette méconnaissance que l'on retrouve dans les dispositions législatives et réglementaires applicables est d'autant plus dommageable que, dans la pratique, les experts en sécurité informatique préconisent l'utilisation systématique de solutions de chiffrement, tant dans le cadre d'un usage courant pour protéger sa vie privée, que dans le cadre d'usages professionnels pour

se prémunir de l'intelligence économique et du vol de données.

La même dichotomie se retrouve au sein de la puissance publique. Ainsi, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) émet régulièrement des recommandations, et œuvre sur le terrain à généraliser l'utilisation des outils de chiffrement.

Très récemment, à l'occasion de la présentation de son rapport 2015, la CNIL a également eu l'occasion de souligner que *« le chiffrement est un élément vital de notre sécurité. Il contribue aussi à la robustesse de notre économie numérique et de ses particules élémentaires que sont les données à caractère personnel, dont la protection est garantie par l'article 8 de la Charte des droits fondamentaux de l'Union européenne »*. Elle ajoute que *« les solutions de chiffrement robustes, sous la maîtrise complète de l'utilisateur, contribuent à l'équilibre et à la sécurité de l'écosystème numérique »* (CNIL, 8 avril 2016, « Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ? »).

Une plus grande utilisation des outils de chiffrement est également préconisée par différentes instances européennes. Ainsi, entre autres documents, une note de l'ENISA du 20 janvier 2016 se montre clairement en faveur du chiffrement aussi bien pour un usage courant que pour un usage professionnel. En effet, ce dernier souligne que *« des services numériques vulnérables ne sont pas seulement un risque pour la société civile. Dans l'Agenda numérique pour l'Europe, il a été souligné que la confiance dans les technologies de l'information est de la plus haute importance. La nouvelle directive sur la sécurité des réseaux et de l'information doit « permettre [...] au public et au secteur privé de faire confiance à des services permis par les réseaux numériques au niveau national et européen. En définissant des incitations pour favoriser les investissements, la transparence et la sensibilisation des utilisateurs, la stratégie choisie stimulera la compétitivité, la croissance et l'emploi dans l'UE » »* (traduction libre de ENISA, « On the free use of cryptographic tools for (self) protection of EU citizens », Enisa.europa.eu, 20 janvier 2016 – A ce sujet et pour d'autres illustrations, voir l'*amicus curiae* des associations exposantes, pp. 47 et s. – **Prod. 2 de la requête introductive**)

Dans ces conditions, tout comme pour les métadonnées, fixer une durée de conservation infiniment plus longue pour les données chiffrées revient à réaliser une différence qui n'est en aucun cas fondée « sur un critère objectif » au sens des exigences de la Cour de justice de (*Digital Rights Ireland*, précité, § 63 et 64).

En tout état de cause, la durée considérable de conservation fixée à six ans est radicalement disproportionnée, d'autant qu'il convient de rappeler qu'un tel chiffrage peut simplement être le fait de personnes qui se sont bornées à suivre les recommandations de l'ANSSI, de la CNIL et de l'INRIA en matière de sécurité et aucunement de « *personnes [qui] se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales* » (*Digital Rights*, précité, § 60).

En somme, ces données chiffrées sont conservées durant une longue période de six ans sans « *aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique* » (*Ibid.*), au mépris des exigences de la Charte.

Sur la conservation des données personnelles des professionnels protégés

XIX-2.3 En outre, il y a lieu de relever que les professionnels protégés n'échappent pas à cette conservation disproportionnée, faute de toute garantie légale en ce sens et alors même que le chiffrage des courriels n'inclut pas celui des données techniques qui permettent de savoir si la personne concernée est un professionnel protégé.

Pourtant, la Cour de justice a fermement souligné que toute mesure qui « ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel » porte atteinte au droit au respect de la vie privée (*Digital Rights Ireland*, précité, § 58).

Sur la conservation de données pour les besoins de l'analyse technique

XIX-2.4 Au surplus, le dernier alinéa de l'article L. 822-2, I, du code

de la sécurité intérieure dispose que les données qui, par définition, relèvent du contenu et non de la métadonnée, peuvent être conservées sans aucune limite pour des usages autres que la surveillance des personnes concernées.

En effet, si cette conservation peut être envisagée pour les données qui « *contiennent des éléments de cyberattaque* » et sont donc constitutifs des éléments matériels d'une infraction, les mots « *ou qui sont chiffrés ainsi que les renseignements déchiffrés associés à ces derniers* » étendent ce dispositif de conservation « *au-delà des durées mentionnées au présent I* » sans justification, s'agissant de données qui ne sont pas, *a priori*, en lien avec quelque infraction que ce soit.

Les données de tout un chacun peuvent donc, si elles sont chiffrées ou ont été déchiffrées, être conservées pour une durée accrue, voire sans aucune limite temporelle. Cette extension est là encore manifestement disproportionnée et imprévisible, dès lors qu'aucune durée de conservation n'est prévue et que ni la loi, ni même ses décrets d'application, n'ont prévu l'anonymisation de ces données éminemment personnelles.

Par conséquent, le régime de conservation des données ainsi mis en place par le cinquième alinéa de l'article L. 822-2 du code de la sécurité intérieure – lequel régime déroge donc aux durées de conservation fixées en principe en prévoyant une durée de conservation illimitée des renseignements – méconnaît manifestement les exigences européennes relatives au droit au respect de la vie privée et au droit au respect du secret des communications des personnes (v. en particulier *Digital Rights*, précité, § 60 ; dans le même sens, v. aussi Cour EDH, 3^e Sect. 29 juin 2006, *Weber et Saravia c. Allemagne*, Req. n° 54934/00, § 95).

Un tel constat ne saurait être infirmé par l'idée selon laquelle la conservation illimitée de ces informations et documents est justifiée par le besoin de leur « *analyse technique* ». En effet, il importe de rappeler que les éléments concernés sont des données et communications chiffrées ou ayant été déchiffrées. Or, d'un point de vue technique, conserver des données déchiffrées pour leur analyse technique est dénué de sens, puisque leur déchiffrement est l'aboutissement d'une telle analyse technique.

Dès lors, les mots « *ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers* » du sixième alinéa de l'article L. 822-2 du code de la sécurité intérieure méconnaissent notamment les articles 7 et 8 de la Charte.

Sur la conservation de données sans rapport avec l'autorisation d'accès et de collecte

XIX-2.5 Enfin, l'article L. 851-6 du code de la sécurité intérieure prévoit pour les informations et documents n'ayant aucun rapport avec l'autorisation initiale d'accès et de collecte une durée de conservation pouvant aller jusqu'à quatre-vingt-dix jours.

Cette durée de conservation est donc **trois fois supérieure** à celle autorisée pour les « *correspondances interceptées en application de l'article L. 852-1 et pour les paroles captées en application de l'article L. 853-1* », qui ne peuvent être conservées que trente jours à compter de leur recueil.

Pourtant, à la différence de ces dernières, ces données n'ayant aucun rapport avec l'autorisation initiale d'accès et de collecte sont sans importance pour les services de renseignement.

Une fois encore, ces dispositions sont manifestement contraires aux exigences exposées par la Cour de justice, en particulier dans son arrêt *Digital Rights Ireland* par lequel elle a invalidé la Directive sur la conservation des données au motif qu'elle mettait en place une collecte de données de 2006 sans « *aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique* » (*Digital Rights*, précité, § 60).

XIX-3 En définitive, il résulte de ce qui précède que les dispositions législatives contestées de l'article L. 822-2 du code de la sécurité intérieure augmentent considérablement, voire indéfiniment, la durée de conservation des informations et documents recueillis sans justification suffisante et ne peuvent donc être regardées que comme contraires aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union.

A ce sujet également, toute autre interprétation implique nécessairement que le Conseil d'Etat transmette à la Cour de justice de l'Union européenne la question préjudicielle suivante :

« L'exigence tirée des articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne selon laquelle « la détermination de la durée de conservation [de données] doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire » (Digital Rights Ireland, C-293/12 et C-594/12, § 63 et 64) peut-elle être regardée comme satisfaite lorsqu'une législation nationale, d'une part, prévoit une durée de conservations bien plus longue est prévue pour les métadonnées, les données chiffrées et les données sans rapport avec l'autorisation d'accès et de collecte ; d'autre part, prévoit une durée indéfinie concernant les données faisant l'objet d'usages autres que la surveillance des personnes concernées ; et enfin, ne prévoit aucune garantie légale concernant la conservation de données impliquant des professionnels protégés ? »

Sur l'absence de contrôle effectif par une autorité indépendante

XX. De quatrième part, les dispositions légales contestées portent également une atteinte aux droits garantis par les articles 7 et 8 de la Charte faute d'avoir prévu un contrôle effectif des conditions dans lesquelles les techniques de renseignement litigieuses sont mises en œuvre.

En effet, outre la méconnaissance directe du droit à un recours effectif tel que garanti par l'article 47 de la Charte (cf. *infra* au point **XXIII**), une telle absence de contrôle effectif confère un caractère disproportionné aux ingérences contestées au sein du droit au respect de la vie privée et du droit à la protection des données personnelles.

Et ce, tout particulièrement concernant l'absence d'autorisation préalable à la collecte de renseignements.

XX-1 En effet, et en droit, il y a lieu de rappeler que la Cour de justice de l'Union européenne juge que tout « accès aux données » doit, pour ne pas porter des atteintes disproportionnées aux droits fondamentaux

reconnus aux article 7 et 8 de la Charte, être « *subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi* » (cf. CJUE, 8 avril 2014, *Digital Rights Ireland Ltd*, C-293/12, § 62).

XX-2 Or, en l'occurrence, s'agissant d'abord de la collecte des renseignements, l'article L. 821-1 du code de la sécurité intérieure prévoit que la mise en œuvre de technique de collecte est « *soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement* » (CNCTR).

Sont ainsi établis deux contrôles préalables : l'autorisation du Premier ministre – lequel n'est pas une entité administrative indépendante des agents recourant aux mesures, puisque ceux-ci sont précisément sous son autorité – et le contrôle préalable de la CNCTR.

Si cette dernière peut prétendre à la qualité d'entité administrative indépendante, l'avis préalable qu'elle rend n'a aucune force contraignante et ne saurait dès lors être susceptible de « *limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi* » (comp. *Digital Rights Ireland Ltd*, précité, § 62).

Ensuite, s'agissant de l'accès ultérieur aux renseignements collectés par les services, l'article L. 822-3 du code de la sécurité intérieure prévoit que les opérations par lesquelles ces renseignements sont « *transcrits ou extraits [...] sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement* », mais sans les soumettre à aucune décision préalable de cette dernière susceptible de les limiter au strict nécessaire.

XX-3 Partant, faute d'avoir soumis la collecte et l'utilisation secrètes de renseignements à l'autorisation préalable d'une juridiction ou d'une entité administrative indépendante susceptible de limiter ces opérations au strict nécessaire, les articles L. 821-1 et L. 822-3 du code de la sécurité intérieure portent une atteinte disproportionnée aux

droits fondamentaux reconnus aux articles 7 et 8 de la Charte.

Si le Conseil d'Etat devait douter d'une telle atteinte, il lui reviendrait de transmettre à la Cour de justice une question préjudicielle qui pourrait être ainsi libellée :

« Les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant une législation nationale à permettre la collecte et l'utilisation secrète de données à caractère personnel sans soumettre la validité de telles opérations à l'autorisation préalable d'une entité indépendante des autorités habilitées à user des techniques de renseignement ? »

En ce qui concerne la méconnaissance du droit à un recours effectif

XXI. Deuxièmement, les dispositions du livre VIII du code de la sécurité intérieure intitulé « *Du renseignement* » ainsi que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, portent atteinte au droit à un recours effectif et au droit à un procès équitable, dont dérive tout particulièrement le principe du contradictoire, tels que garantis par la Charte des droits fondamentaux de l'Union européenne.

XXII. En effet, et en droit, il importe de souligner que l'article 47 de la Charte prévoit que :

« 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 [...] »

XXII-1 De manière générale, la Cour de justice souligne de jurisprudence constante que « *l'article 47, premier alinéa, de la*

Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit » (CJUE, 6 octobre 2015, Schrems, C-362/14, § 95).

XXII-2 Plus précisément encore, dans le cadre spécifique de la surveillance, la Cour de justice a eu l'occasion de préciser sur le fondement de ces stipulations qu'une « *réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective* » et que « *l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit* » (CJUE, 6 octobre 2015, Schrems, C-362/14, § 95).

En outre, par un autre récent arrêt de Grande chambre, la Cour de justice a souligné que :

« Si, dans des cas exceptionnels, une autorité nationale s'oppose à la communication à l'intéressé des motifs précis et complets qui constituent le fondement d'une décision prise en application de l'article 27 de la directive 2004/38, en invoquant des raisons relevant de la sûreté de l'État, le juge compétent de l'État membre concerné doit avoir à sa disposition et mettre en œuvre des techniques et des règles de droit de procédure permettant de concilier, d'une part, les considérations légitimes de la sûreté de l'État quant à la nature et aux sources des renseignements ayant été pris en considération pour l'adoption d'une telle décision et, d'autre part, 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 » (CJUE, 4 juin 2013, ZZ contre Secretary of State for the Home Department, C-300/11, § 57).

Ainsi, « les États membres sont tenus de prévoir, d'une part, **un**

contrôle juridictionnel effectif tant de l'existence et du bien-fondé des raisons invoquées par l'autorité nationale au regard de la sûreté de l'État que de la légalité de la décision prise en application de l'article 27 de la directive 2004/38 ainsi que, d'autre part, des techniques et des règles relatives à ce contrôle » (Ibid. § 58).

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. § 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 » (Ibid. § 60 et 62).

En tout état de cause, au titre de l'article 47 de la Charte, la Cour de justice exige des Etats qu'ils garantissent la « *protection juridictionnelle effective tout en limitant les ingérences éventuelles dans l'exercice de ce droit au strict nécessaire* » (Ibid. § 64).

XXII-3 En outre, il importe d'apprécier ces exigences tirées de la Charte des droits fondamentaux à l'aune des standards internationaux qui imposent aux autorités publiques de garantir aux personnes un accès aux données qui les concernent et, par exception, de justifier de façon suffisante le caractère non-communicable de certaines données.

Ainsi, selon une bonne pratique établie au sein des Nations Unies :

« Les personnes physiques ont la possibilité de demander à accéder aux données personnelles les concernant détenues par les services de renseignement. Elles peuvent exercer ce droit en adressant une requête aux autorités concernées ou par le biais d'une institution indépendante chargée de la protection ou du contrôle des données. Elles ont le droit de corriger toute erreur contenue dans leurs données personnelles. Les éventuelles exceptions à ces règles générales sont prescrites par la loi, strictement limitées, proportionnées et nécessaires pour permettre aux services de renseignement de remplir leur mandat. Il revient aux services de renseignement de justifier devant une institution de contrôle indépendante toute décision de ne pas communiquer des renseignements personnels » (Nations Unies, Assemblée générale, Conseil des droits de l'homme, Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte antiterroriste, Martin Scheinin, 17 mai 2010, A/HRC/14/46, p. 25 - Pratique n° 26).

XXIII. Or, en l'occurrence, les dispositions légales contestées méconnaissent ces exigences à plusieurs titres.

Sur les limitations de l'accès aux données dans le cadre juridictionnel

XXIV-1 D'abord, il y a lieu de souligner que les dispositions de l'article L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015, prévoient que lorsque le Conseil d'État est saisi d'un recours contre la décision de la CNIL, il « *se fonde sur les éléments contenus, le cas échéant, dans le traitement sans les révéler ni révéler si le requérant figure ou non dans le traitement* ».

En outre, aux termes des dispositions de l'article 41 de la loi n° 78-17 du 6 janvier 1978, « *lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions* » suivantes :

- « *La demande est adressée à la [CNIL] pour mener les investigations utiles et faire procéder aux modifications nécessaires* » ;

- « *Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant* ».

Dans ces conditions, les dispositions légales de l'article L. 773-8 du code de justice administrative font obstacle à l'accès du requérant à ses données lors de son recours juridictionnel, alors même que de telles données ne sont pas nécessairement protégées par le secret défense.

De ce seul chef, les dispositions contestées méconnaissent les exigences dérivées de l'article 47 de la Charte des droits fondamentaux.

Si le Conseil d'Etat devait douter d'une telle atteinte, il lui reviendrait de transmettre à la Cour de justice une question préjudicielle qui pourrait être ainsi libellée :

« L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à interdire, par principe et sans exception aucune, l'accès d'une personne à ses données personnelles ou même à d'autres éléments corrélatifs lorsqu'elle initie un recours relatif au traitement de données devant la juridictions compétente ? »

Mais il y a plus.

Sur l'absence de garanties entourant l'accès aux données transmises par des services étrangers

XXIV-2 Ensuite, les dispositions de l'article L. 773-1 du code de la justice administrative prévoient que, en matière de contestation de la validité d'une technique de surveillance, « *le Conseil d'Etat examine les requêtes présentées sur le fondement des articles L. 841-1* » du code de la sécurité intérieure.

XXIV-2.1 Or, ce dernier article L. 841-1 prévoit, à son 1°, que le

Conseil d'État peut être saisi par « *toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4* ».

Ainsi, ces personnes ne peuvent le saisir sans apporter une telle justification.

L'article L. 833-4 du même code qui définit cette procédure prévoit que « *lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la [CNCTR] procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre* » (soit le livre VIII du code de la sécurité intérieure).

Or, l'article L. 833-2 prévoit, à son 4°, que, « *pour l'accomplissement de ses missions, la commission [...] peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions, y compris lorsque la technique de recueil de renseignement mise en œuvre n'a fait l'objet ni d'une demande, ni d'une autorisation ou ne répond pas aux conditions de traçabilité, à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux* ».

XXIV-2.2 Ainsi, toute personne souhaitant contester devant le Conseil d'État la validité du recueil de renseignements la concernant auprès de services étrangers, ou contester la validité de l'exploitation de ces renseignements, ne pourrait justifier « *de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4* », la CNCTR n'étant pas autorisée à procéder « *au contrôle de la ou des techniques invoquées* ».

Ainsi, les personnes concernées par le recueil et l'exploitation de renseignements transmis par des services étrangers ne disposent d'aucun recours juridictionnel pour en contester la validité. Et ce, alors que les échanges de données entre les agences de différents pays constituent une modalité centrale des formes contemporaines du renseignement.

L'atteinte au droit à un recours effectif est d'autant plus manifeste et radicale qu'à l'instar de ce qui est prévu pour les mesures de surveillance internationale – elles-mêmes non assorties d'un dispositif suffisant de recours effectif –, le législateur n'a prévu strictement aucune voie permettant à la CNCTR de contester les mesures en cause.

En effet, l'article L. 854-9 du code de la sécurité intérieure consacré aux mesures de surveillance internationale et issu de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales prévoit que « *lorsqu'elle constate un manquement au présent chapitre, la commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse* » et que, lorsque « *le Premier ministre ne donne pas suite à cette recommandation ou que les suites qui y sont données sont estimées insuffisantes, le Conseil d'Etat [...] peut être saisi par le président ou par au moins trois membres de la commission* ».

Or, s'agissant des mesures relatives aux renseignements recueillis auprès de services étrangers, la CNCTR ne peut user d'une telle voie, faute d'être informée de leur existence, d'être autorisée à en prendre connaissance par elle-même ou encore d'être légalement habilitée à émettre une recommandation au Premier ministre qui pourrait être le préalable à une saisine du Conseil d'État.

XXIV-2.3 Une telle carence manifeste quant à l'existence même de voies de recours effectives est d'autant plus grave que le recueil de renseignements auprès de services étrangers n'est encadré par aucune garantie légale.

En effet, le législateur a totalemment omis de prévoir les finalités d'une telle pratique, les renseignements qu'elle est susceptible de concerner, leur durée de conservation ou encore la présence d'un quelconque contrôle préalable par une autorité indépendante.

Une telle absence de toute garantie en matière de recueil de renseignements auprès de services étrangers – combinée aux très faibles garanties qui entourent l'interception par les services français de communications internationales – revient à autoriser les agences de renseignement en Europe, dont les services français, à contourner les

contraintes légales prévues dans chaque Etat.

En effet, les agences d'un Etat donné peuvent ainsi collecter en masse, dans un cadre juridique fort peu contraignant, des données concernant la population d'États alliés. Et ce, pour ensuite les transmettre aux autorités de ces Etats sans que celles-ci n'aient à respecter leurs contraintes internes respectives. Le tout, réciproquement, puisqu'il n'est guère difficile d'imaginer que l'Etat ayant ainsi partagé des données concernant ses homologues puisse obtenir, en retour, des données liées à sa propre population sans avoir à se soumettre aux exigences de son propre ordre juridique.

Concrètement, le GCHQ britannique ou le BND allemand peuvent ainsi collecter les communications de résidents français en vertu de dispositions qui, dans leur droit national respectif, relèvent de la surveillance des communications internationales, puis les transférer à leurs homologues français de la DGSE, lesquels échappent alors à tout encadrement et contrôle quant à l'utilisation de ces données.

XXIV-2.4 Partant, en privant les personnes concernées de tout recours juridictionnel contre le recueil et l'exploitation par les services français de renseignements transmis par des services étrangers, les dispositions de l'article L. 833-2, 4°, du code de la sécurité intérieure méconnaissent radicalement les exigences de l'article 47 de la Charte des droits fondamentaux.

Là encore, si le Conseil d'Etat devait douter d'une telle conclusion, il lui reviendrait nécessairement de soumettre à la Cour de justice de l'Union européenne une question préjudicielle ainsi libellée :

« L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à priver les justiciables de toute voie de recours juridictionnel pour contester la validité de la collecte et de l'exploitation par les services de renseignements de l'Etat concerné de données communiquées par les services d'un autre État, sans même prévoir un quelconque autre contrôle par une entité indépendante ? »

Sur la méconnaissance du principe du contradictoire

XXIV-3 De plus, les conditions dans lesquelles les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ont institué le contrôle juridictionnel du Conseil d'Etat concernant les techniques de renseignement méconnaissent les exigences du droit au recours effectif et au procès équitable, tout particulièrement le principe corrélatif du contradictoire.

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.

XXIV-3.1 En effet, il y a lieu de souligner que l'article L. 773-6 du code de la justice administrative 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. »

En outre, les dispositions de l'article L. 773-7 du code de la justice administrative 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. »

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

XXIV-3.2 Or, il convient de rappeler que l'article 413-9 du code pénal dispose que :

« Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat. »

Ainsi, et d'une part, aucune définition légale ne détermine avec les précisions nécessaires le champ matériel de la notion de « *secret de la défense nationale* ».

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), synthétisée 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 »

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.

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'arrêté 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 ».

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).

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.

XXIV-3.3 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 du code de justice administrative, 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 de l'obligation pour « *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 éléments liés aux techniques litigieuses de renseignement, que 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 par l'autorité nationale compétente et [...] doit apprécier, conformément aux règles de procédure nationales, si la sûreté de l'État s'oppose à une telle communication* » (CJUE, 4 juin 2013, *ZZ contre Secretary of State for the Home Department*, C-300/11, § 60 et 62).

En définitive, les dispositions légales contestées portent radicalement atteinte au droit au recours effectif ainsi qu'aux exigences du droit à un procès équitable, tel que garantis à l'article 47 de la Charte des droits fondamentaux.

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.

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

XXIV-4 Enfin, et corrélativement, les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative 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.

XXIV-4.1 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'Etat 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.

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.

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.

XXIV-4.2 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.

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.

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* ».

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).

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).

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.

Enfin, la seule circonstance que, selon les dispositions de l'article L. 773-5 du code de justice administrative, le juge compétent puisse soulever tout moyen d'office ne saurait compenser un tel déséquilibre profond.

XXIV-4.3 Une telle conclusion s'impose d'autant qu'à l'instar de l'ensemble des garanties prévues par la Charte, il y a lieu d'apprécier les exigences de l'article 47 de la Charte à l'aune de la jurisprudence de la Cour européenne des droits de l'homme (cf. *supra* au point **XIII**).

Or, dans son arrêt *Kennedy c. Royaume-Uni* du 18 mai 2010 relatif à des mesures de surveillance secrète, la Cour européenne des droits de l'homme a certes souligné qu'elle « *souscri[vait] 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. Royaume-Uni*, Req. n° 26839/05, § 187).

Toutefois, 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, absent dans la procédure ici instituée.

XXIV-4.4 En définitive, les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative portent atteinte de manière disproportionnée aux droits et principes garantis par l'article 47 de la Charte.

XXIV-5 Si le Conseil d'Etat devait douter des conclusions précédentes (cf. *supra* aux points **XXIV-3** et **XXIV-4**), il lui reviendrait nécessairement de renvoyer à la Cour de justice la question préjudicielle suivante :

« 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'une Etat 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 ? »

XXV. Il résulte de tout ce qui précède que les dispositions du livre VIII du code de la sécurité intérieure ainsi que les articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, méconnaissent notamment les articles 7, 8, 20 et 47 de la Charte des droits fondamentaux de l'Union européenne.

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

Sur la méconnaissance de la directive 2000/31/CE sur le commerce électronique par l'article L. 851-3 du code de la sécurité intérieure

XXVI. En quatrième et dernier lieu, les dispositions du décret contesté sont illégales en l'absence de toute base juridique qui en permettent l'édiction, compte tenu de la contrariété de l'article L. 851-3 du code de la sécurité intérieure que les dispositions réglementaires mettent notamment en œuvre avec la directive 2000/31/CE sur le commerce électronique.

XXVI-1 En effet, et en droit, l'article 15, paragraphe 1, de la directive 2000/31/CE sur le commerce électronique dispose que « *les États*

membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ».

Sur ce fondement, la Cour de justice a déjà jugé qu'une injonction faite à un fournisseur d'accès à internet (FAI) de mettre en œuvre sur son réseau un « *système de filtrage* » en vue de détecter l'échange non autorisé d'œuvres soumises au droit d'auteur et conduisant à « *procéder à une surveillance active de l'ensemble des données concernant tous ses clients [...] imposerait audit FAI une surveillance générale qui est interdite par l'article 15, paragraphe 1, de la directive 2000/31* » (CJUE, 24 novembre 2011, *Scarlet Extended c. SABAM*, C-70/10, §40).

Une même solution a été retenue à propos d'une injonction identique faite à un hébergeur (CJUE, 16 février 2012, *SABAM c. Netlog*, C-360/10, §38).

XXVI-2 Or, en l'occurrence, les dispositions de l'article L. 851-3, I, du code de la sécurité intérieure prévoient que, « *pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* ».

Les opérateurs et personnes mentionnés sont notamment des fournisseurs d'accès à internet (FAI) et des hébergeurs.

Mettre en œuvre sur leurs réseaux un tel traitement automatisé reviendrait techniquement pour chacun d'eux à « *procéder à une surveillance active de l'ensemble des données concernant tous ses clients* », soit donc un système techniquement identique à ceux dont la Cour de justice fut saisie dans les arrêts précités *Scarlet Extended c. SABAM* et *SABAM c. Netlog*.

XXVI-3 Partant, la mise en œuvre des dispositifs techniques visés à l'article L. 851-3 du code de la sécurité intérieure constitue une obligation générale de surveillance imposée aux intermédiaires techniques, en méconnaissance de l'interdiction prévue à l'article 15 § 1 de la directive 2000/31.

Si le Conseil d'État devait douter d'une telle conclusion, il lui reviendrait nécessairement de transmettre la question préjudicielle suivante à la Cour de justice :

« L'article 15 de la directive 2000/31 doit-il être interprété comme autorisant une législation nationale à imposer aux opérateurs, fournisseurs d'accès et hébergeurs la mise en œuvre de dispositifs techniques analysant de manière indiscriminée les données circulant sur leurs infrastructures ? »

PAR CES MOTIFS, et tous autres à produire, déduire, suppléer, au besoin même d'office, les associations exposantes persistent dans les conclusions de leurs précédentes écritures, avec toutes conséquences de droit et concluent, **en outre**, à ce qu'il plaise au Conseil d'Etat :

- le cas échéant, **SAISIR** la Cour de justice de l'Union européenne des questions préjudicielles suivantes :

- 1) *« Une législation nationale – telle que la loi française relative au renseignement en date du 24 juillet 2015 ou celle relative aux mesures de surveillance des communications électroniques internationales du 30 novembre 2015 – qui a pour objet d'autoriser les services de renseignement à recourir à de multiples techniques de surveillance, tel le recueil de données de connexion, relève-t-elle des « mesures législatives visant à limiter la portée des droits et des obligations » au sens de l'article 15.1 de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ; et, corrélativement mais aussi au regard de l'objet même de cette législation, met-elle « en œuvre le droit de l'Union » au sens des stipulations de l'article 51, al. 1er, de la Charte des droits fondamentaux de l'Union européenne de sorte que les droits et libertés prévus notamment par les articles 7 et 8 de cette Charte lui sont opposables ? »*

Corrélativement, l'arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12) doit-il être interprété en ce sens qu'il pose des exigences, au regard des articles 7 et 8 de la Charte, qui s'imposent à un régime national régissant la conservation des données relatives à des communications électroniques et l'accès à de telles données ? »

2.1) *« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant à un État membre de prévoir de façon secrète l'interception de communications privées, la pose de microphones ou de caméras dans des lieux d'habitation ou encore l'usage d'autres dispositifs intrusifs de*

surveillance dans le but de collecter tout renseignement susceptible de défendre ou de promouvoir des intérêts aussi vastes que : - les intérêts majeurs de sa politique étrangère ; - l'exécution de ses engagements européens et internationaux ; - ses intérêts économiques, industriels et scientifiques majeurs ; - la prévention de l'organisation de manifestation non déclarée ou ayant fait l'objet d'une déclaration incomplète ; ou encore - la prévention de l'acquisition ou de l'emploi de stupéfiants à fins de consommation personnelle ? »

2.1) a) *« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant un État membre à collecter de façon indiscriminée et secrète des données techniques concernant l'ensemble des utilisateurs d'un réseau et pouvant être rattachées à ceux-ci ? »*

b) *« Les articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant un État membre à collecter, conserver et exploiter un ensemble de données sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques à ces données ? »*

2.2) *« L'exigence tirée des articles 7, 8 et 52, paragraphe 2, de la Charte des droits fondamentaux de l'Union européenne selon laquelle « la détermination de la durée de conservation [de données] doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire » (Digital Rights Ireland, C-293/12 et C-594/12, § 63 et 64) peut-elle être regardée comme satisfaite lorsqu'une législation nationale, d'une part, prévoit une durée de conservations bien plus longue est prévue pour les métadonnées, les données chiffrées et les données sans rapport avec l'autorisation d'accès et de collecte ; d'autre part, prévoit une durée indéfinie concernant les données faisant l'objet d'usages autres que la surveillance des personnes concernées ; et enfin, ne prévoit aucune garantie légale concernant la conservation de données impliquant des professionnels protégés ? »*

2.3) « *Les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne doivent-ils être interprétés comme autorisant une législation nationale à permettre la collecte et l'utilisation secrète de données à caractère personnel sans soumettre la validité de telles opérations à l'autorisation préalable d'une entité indépendante des autorités habilitées à user des techniques de renseignement ?* »

2.4) a) « *L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à interdire, par principe et sans exception aucune, l'accès d'une personne à ses données personnelles ou même à d'autres éléments corrélatifs lorsqu'elle initie un recours relatif au traitement de données devant la juridictions compétente ?* »

c) « *L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit-il être interprété comme autorisant une législation nationale à priver les justiciables de toute voie de recours juridictionnel pour contester la validité de la collecte et de l'exploitation par les services de renseignements de l'Etat concerné de données communiquées par les services d'un autre État, sans même prévoir un quelconque autre contrôle par une entité indépendante ?* »

d) « *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'une Etat 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 ?* »

3) « *L'article 15 de la directive 2000/31 doit-il être interprété comme autorisant une législation nationale à imposer aux opérateurs, fournisseurs d'accès et hébergeurs la mise en*

œuvre de dispositifs techniques analysant de manière indiscriminée les données circulant sur leurs infrastructures ? »

Ou toute autre formulation qu'il voudra bien lui substituer.

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

Productions :

1. Marc Rees, « Loi Renseignement : le cri d'alarme du surveillant des surveillants », *in NextImpact*, 16 février 2016