

C-5M/18-1

2/1

CONSEIL D'ETAT  
statuant  
au contentieux

CR

N<sup>os</sup> 394922, 394925, 397844, 397851

REPUBLIQUE FRANÇAISE

QUADRATURE DU NET et autres

AU NOM DU PEUPLE FRANÇAIS

IGWAN.NET

M. Vincent Villette  
Rapporteur

Le Conseil d'Etat statuant au contentieux  
(Section du contentieux, 10ème et 9ème chambres réunies)

M. Edouard Crépey  
Rapporteur public

Inscrit au registre de la	
Cour de justice sous le n° <u>4088400</u>	Sur le rapport de la 10ème chambre de la Section du contentieux
Luxembourg, le 08.08.2018	Le Greffier, par ordre
Fax / E-mail: _____	<i>V. Giacobbo</i>
Déposé le: <u>03.08.18</u>	Valérie Giacobbo - Peyronnel Administrateur

Séance du 11 juillet 2018  
Lecture du 26 juillet 2018

1° Sous le numéro 394922, par une requête sommaire, un mémoire complémentaire et trois autres mémoires, enregistrés le 30 novembre 2015, le 29 février 2016 et le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'Etat, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'Etat la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Elles soutiennent :

- que le décret attaqué est irrégulier car il ne correspond ni à la version soumise au Conseil d'Etat, ni à celle adoptée par ce dernier ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée et le droit au recours effectif, respectivement garantis par les articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et, par suite, que ce décret est dépourvu de base légale ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée, le droit à la protection des données personnelles et le droit au recours effectif respectivement garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et, par suite, que ce décret est dépourvu de base légale ;

03.08.2018  
LUXEMBOURG  
CURIA GREFFE

- que l'article L. 851-3 du code de la sécurité intérieure qui constitue la base légale du décret attaqué méconnaît la directive 2000/31/CE du 8 juin 2000 et, par suite, que ce décret est dépourvu de base légale ;

- que le décret attaqué doit être regardé comme étant dépourvu de base légale en raison de la contrariété de l'article 323-8 du code pénal aux articles 6 et 32 de la convention du 23 novembre 2001 sur la cybercriminalité, et aux articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ainsi qu'aux stipulations du premier protocole additionnel à cette convention et, par suite, que ce décret est dépourvu de base légale.

Par deux mémoires en défense, enregistrés le 26 avril et le 4 juillet 2016, le ministre de la défense conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

Par trois mémoires en défense, enregistrés le 27 juin 2016 et les 26 et 28 juin 2018, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

2° Sous le numéro 394925, par une requête sommaire, un mémoire complémentaire et trois autres mémoires, enregistrés le 30 novembre 2015, le 29 février 2016 et le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'Etat, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2015-1211 du 1<sup>er</sup> octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'Etat la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Elles soutiennent :

- que le décret attaqué est irrégulier car il ne correspond ni à la version soumise au Conseil d'Etat, ni à celle adoptée par ce dernier ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée et le droit au recours effectif, respectivement garantis par les articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et, par suite, que ce décret est dépourvu de base légale ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée, le droit à la protection des données personnelles et le droit au recours effectif respectivement garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et, par suite, que ce décret est dépourvu de base légale ;

- que l'article L. 851-3 du code de la sécurité intérieure qui constitue la base légale du décret attaqué méconnaît la directive 2000/31/CE du 8 juin 2000 et, par suite, que ce décret est dépourvu de base légale.

Par un mémoire en défense, enregistré le 13 juin 2016, le garde des sceaux, ministre de la justice, conclut au rejet de la requête. Il soutient que la requête est irrecevable car les associations ne justifient pas d'un intérêt leur donnant qualité pour agir et qu'en tout état de cause, les moyens soulevés ne sont pas fondés.

Par trois mémoires en défense, enregistrés le 27 juin 2016 et les 26 et 28 juin 2018, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

3° Sous le numéro 397844, par une requête sommaire, un mémoire complémentaire et deux autres mémoires, enregistrés le 11 mars 2016, le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'Etat, l'association Igwan.net demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'Etat la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Elles soutiennent :

- que le décret attaqué est irrégulier car il ne correspond ni à la version soumise au Conseil d'Etat, ni à celle adoptée par ce dernier ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée et le droit au recours effectif, respectivement garantis par les articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et, par suite, que ce décret est dépourvu de base légale ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée, le droit à la protection des données personnelles et le droit au recours effectif respectivement garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et, par suite, que ce décret est dépourvu de base légale ;

- que l'article L. 851-3 du code de la sécurité intérieure qui constitue la base légale du décret attaqué méconnaît la directive 2000/31/CE du 8 juin 2000 et, par suite, que ce décret est dépourvu de base légale.

Par deux mémoires en défense, enregistrés le 28 juin 2016 et le 26 juin 2018, le ministre de l'intérieur conclut au rejet de la requête. Il soutient que la requête est irrecevable car l'association requérante ne justifie pas d'un intérêt lui donnant qualité pour agir et, à titre subsidiaire, que les moyens soulevés ne sont pas fondés.

Par trois mémoires en défense, enregistrés le 5 juillet 2016, le 26 juin et 28 juin 2018, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

4° Sous le numéro 397851, par une requête sommaire, un mémoire complémentaire et deux autres mémoires, enregistrés le 11 mars 2016, le 19 mai 2016, le 24 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'Etat, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'Etat la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Elles soutiennent :

- que le décret attaqué est irrégulier car il ne correspond ni à la version soumise au Conseil d'Etat, ni à celle adoptée par ce dernier ;

- que les dispositions législatives qui constituent la base légale du décret attaqué ont été déclarées contraires à la Constitution par le Conseil constitutionnel et, par suite, que ce décret est dépourvu de base légale ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée et le droit au recours effectif, respectivement garantis par les articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et, par suite, que ce décret est dépourvu de base légale ;

- que les dispositions législatives qui constituent la base légale du décret attaqué méconnaissent le droit au respect de la vie privée, le droit à la protection des données personnelles et le droit au recours effectif respectivement garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et, par suite, que ce décret est dépourvu de base légale ;

- que l'article L. 851-3 du code de la sécurité intérieure qui constitue la base légale du décret attaqué méconnaît la directive 2000/31/CE du 8 juin 2000 et, par suite, que ce décret est dépourvu de base légale ;

- que le décret attaqué méconnaît les dispositions des articles L. 851-1 à L. 851-3 du code de la sécurité intérieure pour l'application desquelles il est notamment pris en étendant le champ des données de connexion susceptibles d'être recueillies.

Par un mémoire en défense, enregistré le 26 juin 2018, le ministre de l'intérieur conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

Par trois mémoires en défense, enregistrés le 4 juillet 2016 et les 26 et 28 juin 2018, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens soulevés ne sont pas fondés.

Vu :

- la Constitution, notamment son Préambule et ses articles 61-1 et 62 ;
- le traité sur l'Union européenne ;
- le traité sur le fonctionnement de l'Union européenne ;
- la Charte des droits fondamentaux de l'Union européenne ;
- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;
- la convention du 23 novembre 2001 sur la cybercriminalité ;
- la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- le code de la sécurité intérieure, notamment son livre VIII ;
- la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016 ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Vincent Villette, maître des requêtes,
- les conclusions de M. Edouard Crépey, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Spinosi, Bureau, avocat de la Quadrature du Net, de French Data Network et de la Fédération des fournisseurs d'accès à internet associatifs ;

Considérant ce qui suit :

1. Par trois requêtes, La Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation pour excès de pouvoir, sous le numéro 394922 du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement, sous le numéro 394925 du décret du 1<sup>er</sup> octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat, et sous le numéro 397851 du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. L'association Igwan.net, sous le numéro 397844, demande l'annulation du décret du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure. Ces requêtes présentent à juger les mêmes questions. Il y a lieu de les joindre pour statuer par une seule décision.

Sur les moyens de légalité externe :

2. Lorsque, comme en l'espèce, un décret doit être pris en Conseil d'Etat, le texte retenu par le Gouvernement ne peut être différent à la fois du projet qu'il a soumis au Conseil d'Etat et du texte adopté par ce dernier. Il ressort des copies des minutes de la section de l'intérieur du Conseil d'Etat, telles qu'elles ont été produites au dossier par le Premier ministre, que le texte des quatre décrets attaqués ne contient pas de disposition qui différerait à la fois du projet initial du Gouvernement et du texte adopté par la section. Il s'ensuit que les moyens tirés

de la méconnaissance des règles qui gouvernent l'examen par le Conseil d'Etat des projets de décret doivent être écartés.

Sur les moyens de légalité interne :

En ce qui concerne le moyen tiré de la méconnaissance de l'article L. 851-1 du code de la sécurité intérieure par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement :

3. Les dispositions de l'article R. 851-5 du code de la sécurité intérieure créées par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement qui définissent les données de connexion susceptibles d'être recueillies auprès des opérateurs de communications électroniques excluent des données ainsi recueillies le contenu des correspondances échangées ou des informations consultées. En outre, ces dispositions réservent le recueil de certaines de ces données aux seules techniques de renseignement prévues aux articles L. 851-2 et L. 851-3 du code de la sécurité intérieure, lesquelles ne sont mises en œuvre que pour les seuls besoins de la prévention du terrorisme. Ce faisant, contrairement à ce que soutiennent les associations requérantes, ces dispositions réglementaires ne méconnaissent pas les dispositions de l'article L. 851-1 du même code pour l'application desquelles elles ont été prises.

En ce qui concerne les moyens invoqués par la voie de l'exception :

4. A l'appui de leurs conclusions, les requérants soulèvent des moyens, par la voie de l'exception, à l'encontre de l'ensemble des dispositions du livre VIII du code de la sécurité intérieure, de celles du chapitre III bis du titre VII du livre VII du code de justice administrative et de celles de l'article 323-8 du code pénal.

S'agissant du moyen tiré de la contrariété à la Constitution de l'article L. 811-5 du code de la sécurité intérieure :

5. Par sa décision n° 2016-590 QPC du 21 octobre 2016, le Conseil constitutionnel a déclaré l'article L. 811-5 du code de la sécurité intérieure contraire au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789. Le dispositif de cette décision énonce que la déclaration d'inconstitutionnalité prend effet dans les conditions prévues aux paragraphes 11 et 12. Aux termes de ces paragraphes : *« L'abrogation immédiate de l'article L. 811-5 du code de la sécurité intérieure aurait pour effet de priver les pouvoirs publics de toute possibilité de surveillance des transmissions empruntant la voie hertzienne. Elle entraînerait des conséquences manifestement excessives. Afin de permettre au législateur de remédier à l'inconstitutionnalité constatée, il y a donc lieu de reporter au 31 décembre 2017 la date de cette abrogation. / Afin de faire cesser l'inconstitutionnalité constatée à compter de la publication de la présente décision, il y a lieu de juger que, jusqu'à l'entrée en vigueur d'une nouvelle loi ou, au plus tard, jusqu'au 30 décembre 2017, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être interprétées comme pouvant servir de fondement à des mesures d'interception de correspondances, de recueil de données de connexion ou de captation de données informatiques soumises à l'autorisation prévue au titre II ou au chapitre IV du titre V du livre VIII du code de la sécurité intérieure. Pendant le même délai, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être mises en œuvre sans que la Commission nationale de contrôle des techniques de renseignement soit régulièrement informée sur le champ et la nature des mesures prises en application de cet article »*. Alors même que, selon les motifs de la

décision du Conseil constitutionnel, la déclaration d'inconstitutionnalité doit, en principe, bénéficier à l'auteur de la question prioritaire de constitutionnalité, l'absence de prescriptions relatives à la remise en cause des effets produits par l'article L. 811-5 du code de la sécurité intérieure avant son abrogation doit, en l'espèce, eu égard, d'une part, à la circonstance que la question prioritaire de constitutionnalité a été soulevée à l'occasion de recours pour excès de pouvoir dirigés contre des actes réglementaires, d'autre part, à la circonstance que le Conseil constitutionnel a décidé de reporter dans le temps les effets abrogatifs de sa décision, être regardée comme indiquant que le Conseil constitutionnel n'a pas entendu remettre en cause les effets que la disposition déclarée contraire à la Constitution avait produits avant la date de son abrogation. Il s'ensuit que, alors même que les associations requérantes sont les auteurs de la question prioritaire de constitutionnalité, la déclaration d'inconstitutionnalité de l'article L. 811-5 du code de la sécurité intérieure est, en tout état de cause, sans incidence sur l'issue des présents litiges dirigés contre les quatre décrets mentionnés au point 1.

S'agissant de l'exception d'inconstitutionnalité dirigée contre l'article 323-8 du code pénal :

6. La contrariété d'une disposition législative aux stipulations d'un traité international ne peut être utilement invoquée à l'appui de conclusions dirigées contre un acte réglementaire que si ce dernier a été pris pour son application ou si en elle constitue la base légale. Or, le décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement n'a été pris ni sur le fondement ni pour l'application des dispositions de l'article 323-8 du code pénal. Il s'ensuit que les associations requérantes ne peuvent utilement soutenir que ce décret serait dépourvu de base légale en raison de la contrariété des dispositions de l'article 323-8 du code pénal aux stipulations des articles 6 et 32 de la convention du 23 novembre 2001 sur la cybercriminalité et à celles des articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que de l'article 1<sup>er</sup> du premier protocole additionnel à cette convention.

S'agissant des moyens tirés de la méconnaissance de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :

7. En premier lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit à un recours effectif garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison des atteintes portées au droit au recours, aux droits de la défense et au principe du contradictoire dans le cadre du contentieux de la mise en œuvre des techniques de renseignement.

8. Les dispositions des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure prévoient les conditions dans lesquelles le Conseil d'Etat est compétent pour connaître des requêtes concernant la mise en œuvre des techniques de renseignement soumises à autorisation. Il peut être saisi soit par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre et justifiant d'avoir au préalable saisi la Commission nationale de contrôle des techniques de renseignement sur le fondement de l'article L. 833-4 du même code, soit par le président de cette commission, ou trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes. S'agissant des mesures de surveillance des communications électroniques internationales encadrées par le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, si la personne qui pense faire l'objet d'une telle mesure de surveillance ne peut directement saisir un juge pour en

contester la régularité, elle peut en revanche, sur le fondement des dispositions de l'article L. 854-9 de ce code, former une réclamation à cette fin auprès de la Commission nationale de contrôle des techniques de renseignement. Or, ce même article prévoit que lorsque la commission identifie un manquement, de sa propre initiative ou à la suite d'une telle réclamation, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin et que les renseignements collectés soient, le cas échéant, détruits. Elle peut également saisir le Conseil d'Etat.

9. Saisie de conclusions tendant à ce qu'elle s'assure qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à l'égard du requérant ou de la personne concernée, il appartient à la formation spécialisée, créée par l'article L. 773-2 du code de justice administrative, de vérifier, au vu des éléments qui lui ont été communiqués hors la procédure contradictoire, si le requérant fait ou non l'objet d'une telle technique. Dans l'affirmative, il lui appartient d'apprécier si cette technique est mise en œuvre dans le respect du livre VIII du code de la sécurité intérieure. Lorsqu'il apparaît soit qu'aucune technique de renseignement n'est mise en œuvre à l'égard du requérant, soit que cette mise en œuvre n'est entachée d'aucune illégalité, la formation de jugement informe le requérant de l'accomplissement de ces vérifications et qu'aucune illégalité n'a été commise, sans autre précision. Dans le cas où une technique de renseignement est mise en œuvre dans des conditions qui apparaissent entachées d'illégalité, elle en informe le requérant, sans faire état d'aucun élément protégé par le secret de la défense nationale. En pareil cas, par une décision distincte dont seule l'administration compétente et la Commission nationale de contrôle des techniques de renseignement sont destinataires, la formation spécialisée annule le cas échéant l'autorisation et ordonne la destruction des renseignements irrégulièrement collectés.

10. La dérogation apportée, par les dispositions contestées du code de justice administrative, au caractère contradictoire de la procédure juridictionnelle, qui a pour seul objet de porter à la connaissance des juges des éléments couverts par le secret de la défense nationale et qui ne peuvent, dès lors, être communiqués au requérant, permet à la formation spécialisée, qui entend les parties, de statuer en toute connaissance de cause. Les pouvoirs dont elle est investie, pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées garantissent l'effectivité du contrôle juridictionnel qu'elle exerce.

11. Il s'ensuit que ni les conditions dans lesquelles la formation spécialisée peut être saisie ni celles dans lesquelles elle remplit son office juridictionnel ne méconnaissent, contrairement à ce qui est soutenu, le droit au recours effectif des personnes qui la saisissent, garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

12. En second lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit au respect de la vie privée garanti notamment par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison de l'absence de notification des mesures de surveillance aux personnes concernées après qu'elles ont été levées.

13. Eu égard, d'une part, aux attributions de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante à laquelle il appartient de vérifier, sous le contrôle du juge, que les techniques de recueil de renseignement sont mises en œuvre, sur le territoire national, conformément aux exigences découlant du code

de la sécurité intérieure, et, d'autre part, au recours effectif ouvert, dans les conditions décrites aux points précédents, devant la formation spécialisée du Conseil d'Etat, la circonstance que les dispositions législatives contestées ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet, une fois ces dernières levées, ne caractérise pas, par elle-même, une atteinte excessive portée au droit au respect de la vie privée.

14. Il résulte de ce qui précède que les moyens tirés de la contrariété des dispositions législatives contestées aux articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales doivent, en tout état de cause, être écartés.

S'agissant du moyen tiré de la méconnaissance de la directive du 8 juin 2000 :

15. Les dispositions de l'article L. 851-3 du code de la sécurité intérieure permettent d'imposer aux opérateurs de communications électroniques et aux prestataires techniques « *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* ». Cette technique vise uniquement à recueillir pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces personnes, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, ces dispositions, qui n'imposent pas une obligation générale de surveillance active, ne méconnaissent pas les dispositions claires de l'article 15 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui prévoient que « *Les Etats membres ne doivent pas imposer aux prestataires, pour la fourniture des services de simple transport, de stockage et d'hébergement 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* ». Il s'ensuit qu'en tout état de cause, le moyen tiré de la méconnaissance de la directive du 8 juin 2000 doit être écarté.

S'agissant des moyens tirés de la méconnaissance de la directive du 12 juillet 2002 et de la Charte des droits fondamentaux de l'Union européenne :

16. D'une part, aux termes de l'article 4 du Traité sur l'Union européenne, l'Union « *respecte les fonctions essentielles de l'Etat, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque Etat membre* ». L'article 51 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. (...) 2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités* ». Aux termes de son article 54 : « *Aucune des dispositions de la présente Charte ne doit être interprétée comme impliquant un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Charte (...)* ».

17. D'autre part, la directive 2002/58/CE du Parlement européen et du Conseil 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, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des Etats membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le « *traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté* ». Mais, ainsi que le rappelle son article 1<sup>er</sup>, paragraphe 3, elle « *ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* ». Par ailleurs, son article 15 prévoit que « *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* ». Les Etats membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive.

Quant au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 :

18. Il résulte des dispositions précitées de la directive du 12 juillet 2002, ainsi que l'a dit pour droit la Cour de justice de l'Union européenne par son arrêt *Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres* (C-203/15 et C-698/15), du 21 décembre 2016, qu'elle « doit être regardée comme régissant les activités des fournisseurs [de services de communications électroniques] ». Les dispositions imposant des obligations à ces fournisseurs, telles que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation de leurs utilisateurs et abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de la directive du 12 juillet 2002, parmi lesquelles figure la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique relèvent dès lors du champ d'application de cette directive dans la mesure où, ainsi que l'a dit pour droit la Cour de justice, elles régissent leur activité. Par ailleurs, ainsi que l'a également dit pour droit la Cour, la circonstance que de telles obligations n'interviennent qu'aux seules fins de rendre accessibles aux autorités nationales compétentes les données personnelles qu'elles concernent, implique que la réglementation nationale encadrant l'accès et l'utilisation de ces données relève également du champ d'application de la directive du 12 juillet 2002. En revanche, les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en œuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive.

19. L'article L. 851-1 du code de la sécurité intérieure dispose que : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications (...)* ». Les articles L. 851-2 et L. 851-4 du code de la sécurité intérieure organisent, pour des finalités et selon des modalités différentes, des accès administratifs en temps réel aux données de connexion ainsi conservées.

20. Il résulte clairement de ce qui précède, eu égard au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 tel qu'interprété par la Cour de justice de l'Union européenne, qu'en relèvent tant l'obligation de conservation induite par les dispositions précitées de l'article L. 851-1 du code de la sécurité intérieure que les accès administratifs aux données de connexion, y compris en temps réel, qui la justifient, prévus aux articles L. 851-1, L. 851-2 et L. 851-4 de ce code. Il en va de même des dispositions de l'article L. 851-3 du code de la sécurité intérieure qui, si elles ne font pas peser sur les opérateurs et personnes concernés une obligation préalable de conservation, leur imposent cependant de mettre en œuvre sur leurs réseaux des traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste.

21. En revanche, il résulte clairement de la directive du 12 juillet 2002 que ne relèvent pas de son champ les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure, dès lors qu'elles portent sur des techniques de recueil de renseignement qui sont directement mises en œuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Dès lors, ces dispositions ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.

#### Quant à l'obligation de conservation généralisée et indifférenciée :

22. Par son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a dit pour droit que l'article 15, paragraphe 1, de cette directive, « lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

23. D'une part, il est constant qu'une telle conservation préventive et indifférenciée permet aux services de renseignement d'accéder aux données relatives aux communications qu'un individu a effectuées avant que soient identifiées les raisons de penser qu'il présente une menace pour la sécurité publique, la défense ou la sûreté de l'Etat. Dans un

contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir seulement du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'Etat.

24. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « contenu essentiel » des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits « n'apparaissent pas comme étant des prérogatives absolues » et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que « la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui » et que « l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ».

25. Dans ces conditions, la question de déterminer si l'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit pas être regardée, notamment eu égard aux garanties et contrôles, évoqués aux points 7 à 13, dont sont assortis les accès administratifs aux données de connexion et l'utilisation de celles-ci, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne, soulève une première difficulté d'interprétation du droit de l'Union européenne.

Quant aux autres obligations susceptibles d'être imposées aux fournisseurs d'un service de communications électroniques :

26. Les dispositions de l'article L. 851-2 du code de la sécurité intérieure autorisent, pour les seuls besoins de la prévention du terrorisme, le recueil des informations ou documents prévus à l'article L. 851-1, auprès des mêmes personnes. Ce recueil, qui ne concerne qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste, s'effectue en temps réel. Il en va de même des dispositions de l'article L. 851-4 du même code, qui autorisent la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux. Il suit de là que ces techniques ne font pas peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui est nécessaire à la facturation de leurs services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée. Par ailleurs, ainsi qu'il a été rappelé au point 15, les dispositions de l'article L. 851-3 du code de la sécurité intérieure n'impliquent pas davantage une conservation généralisée et indifférenciée.

27. Or, d'une part, il est constant que les accès en temps réel aux données de connexion permettent de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public. D'autre part, la technique prévue à l'article L. 851-3 du code de la sécurité intérieure permet de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements, notamment compte tenu de leurs modes de communication, sont susceptibles de révéler une menace terroriste. Dans un contexte marqué par des menaces graves et persistantes pour la sécurité

nationale, tenant en particulier au risque terroriste, ces techniques présentent ainsi une utilité opérationnelle sans équivalent.

28. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « contenu essentiel » des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits « n'apparaissent pas comme étant des prérogatives absolues » et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que « la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui » et que « l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ».

29. Dans ces conditions, soulève une deuxième difficulté sérieuse d'interprétation du droit de l'Union européenne la question de déterminer si la directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit être interprétée en ce sens qu'elle autorise des mesures législatives relevant d'activités concernant la sécurité publique, la défense et la sûreté de l'Etat telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données.

Quant à l'accès des autorités nationales compétentes aux données conservées :

30. Dans son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a également dit pour droit que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 « doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union. ». La Cour a, à cette occasion, estimé « qu'il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits ».

31. Soulève une troisième difficulté sérieuse d'interprétation du droit de l'Union la question de déterminer si la directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres

garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours.

32. Les trois questions énoncées aux points 25 à 31 sont déterminantes pour la solution des litiges que doit trancher le Conseil d'Etat sur les quatre décrets attaqués en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure. Elles présentent, ainsi qu'il a été dit, plusieurs difficultés sérieuses d'interprétation du droit de l'Union européenne. Il y a lieu, par suite, d'en saisir la Cour de justice de l'Union européenne en application de l'article 267 du traité sur le fonctionnement de l'Union européenne et, jusqu'à ce que celle-ci se soit prononcée, de surseoir à statuer, dans cette mesure et sans qu'il soit besoin de statuer sur les fins de non-recevoir opposées en défense, sur les requêtes des associations requérantes et de rejeter le surplus de leurs conclusions.

#### DECIDE :

-----

Article 1<sup>er</sup> : Les requêtes sont rejetées en tant qu'elles sont dirigées contre les décrets n° 2015-1185 du 28 septembre 2015, n° 2015-1211 du 1<sup>er</sup> octobre 2015, n° 2015-1639 du 11 décembre 2015 et n° 2016-67 du 29 janvier 2016 en tant qu'ils mettent en œuvre les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure.

Article 2 : Il est sursis à statuer, dans cette mesure, sur les requêtes des associations requérantes, jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions suivantes :

1° L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne ?

2° La directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données ?

3° La directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours ?

Article 3 : La présente décision sera notifiée à la Quadrature du Net, à l'association Igwan.net, au Premier ministre, au ministre d'Etat, ministre de l'intérieur, à la Garde des sceaux, ministre de la justice, à la ministre des armées et au greffier de la Cour de justice de l'Union européenne. Les autres requérantes seront informées de la présente décision par la SCP Spinosi & Sureau, avocat au Conseil d'Etat et à la Cour de cassation, qui les représente devant le Conseil d'Etat.

Délibéré à l'issue de la séance du 11 juillet 2018 où siégeaient : M. Jean-Denis Combrexelle, président de la Section du contentieux, présidant ; M. Mattias Guyomar, M. Guillaume Goulard, présidents de chambre ; M. Philippe Josse, M. Laurent Olléon, Mme Nathalie Escaut, conseillers d'Etat ; M. Vincent Villette, maître des requêtes-rapporteur.

Lu en séance publique le 26 juillet 2018

Le Président :  
Signé : M. Jean-Denis Combrexelle

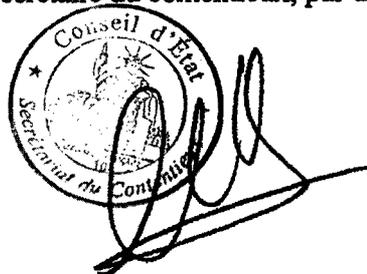
Le rapporteur :  
Signé : M. Vincent Villette

Le secrétaire :  
Signé : Mme Laureen Le Bras

La République mande et ordonne au Premier ministre en ce qui le concerne ou à tous huissiers de justice à ce requis en ce qui concerne les voies de droit commun contre les parties privées, de pourvoir à l'exécution de la présente décision.

Pour expédition conforme,

Pour le secrétaire du contentieux, par délégation :



The image shows a circular official stamp of the Conseil d'Etat, specifically the Secrétariat du Contentieux. The stamp features a central emblem with a sunburst and a scale of justice. The text 'Conseil d'Etat' is at the top and 'Secrétariat du Contentieux' is at the bottom. A handwritten signature in black ink is written over the stamp.