CONSEIL D'ETAT DP
statuant
au contentieux

N^os^ 393099, 394922, 397844, 397851, 424717, 424718

REPUBLIQUE FRANÇAISE

_____

AU NOM DU PEUPLE FRANÇAIS

FRENCH DATA NETWORK et autres

_____

M. Réda Wadjinny-Green
Rapporteur

Le Conseil d'Etat statuant au contentieux

_____

M. Alexandre Lallet
Rapporteur public

Sur le rapport de la 10ème chambre
de la section du contentieux

_____

Séance du 16 avril 2021
Décision du 21 avril 2021

_____

Vu les procédures suivantes :

1° Sous les n^os^ 394922, 397844 et 397851, par une décision du 26 juillet 2018, le Conseil d'Etat, statuant au contentieux sur les requêtes de l'association La Quadrature du Net et autres et de l'association Igwan.net tendant à l'annulation pour excès de pouvoir des décrets n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, 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 de ce code et n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, a sursis à statuer 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 ?

Par un arrêt C-511/18, C-512/18, C520/18 du 6 octobre 2020, la Cour de justice de l'Union européenne s'est prononcée sur ces questions.

Par un nouveau mémoire en défense et trois nouveaux mémoires, enregistrés les 21 janvier, 8 mars, 7 avril et 9 avril 2021, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens tirés, par la voie de l'exception, de l'inconventionnalité des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure ne sont pas fondés dès lors, premièrement, qu'il sont inopérants, deuxièmement, que la réponse apportée par la Cour de justice de l'Union européenne aux questions préjudicielles qui lui étaient posées a manifestement méconnu le principe d'attribution prévu à l'article 5 du traité sur l'Union européenne en empiétant sur les compétences appartenant aux Etats membres en vertu de l'article 4 paragraphe 2 de ce traité et, troisièmement, que cette réponse n'est pas de nature à garantir l'effectivité des objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des infractions et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme, composante de l'objectif de valeur constitutionnelle de protection de l'ordre public.

Par trois nouveaux mémoires, enregistrés les 15 mars, 29 mars et 7 avril 2021, les associations requérantes persistent dans leurs conclusions et soulèvent un nouveau moyen tiré de ce que l'article L. 811-4 dont les décrets attaqués font application méconnaît le droit à la vie privée garanti par la Charte des droits fondamentaux de l'Union européenne dès lors qu'il ne limite pas le nombre de personnes pouvant recourir aux techniques de renseignement listées aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure. Elles demandent en outre au Conseil d'Etat d'enjoindre au Premier ministre de procéder à l'abrogation demandée sous astreinte de 50 000 euros par jour de retard et de mettre à la charge de l'Etat une somme de 31 415 euros au titre de l'article L. 761-1 du code de justice administrative.

2° Sous le n° 393099, par une décision du 26 juillet 2018, le Conseil d'Etat, statuant au contentieux sur la requête de l'association French Data Network et autres tendant à l'annulation pour excès de pouvoir de la décision implicite de rejet résultant du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant

contribué à la création d'un contenu mis en ligne, a sursis à statuer 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, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, 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°) Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un Etat d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ?

Par un arrêt C-511/18, C-512/18, C520/18 du 6 octobre 2020, la Cour de justice de l'Union européenne s'est prononcée sur ces questions.

Par un nouveau mémoire en défense et trois nouveaux mémoires, enregistrés les 21 janvier, 8 mars, 7 avril et 9 avril 2021, le Premier ministre conclut au rejet de la requête. Il soutient que les moyens tirés, par la voie de l'exception, de l'inconventionnalité des articles L. 34-1 du code des postes et communications électroniques et du II de l'article 6 de la loi du 21 juin 2004 ne sont pas fondés dès lors, d'une part, que la réponse apportée par la Cour de justice de l'Union européenne aux questions préjudicielles qui lui étaient posées a manifestement méconnu le principe d'attribution prévu à l'article 5 du traité sur l'Union européenne en empiétant sur les compétences appartenant aux Etats membres en vertu de l'article 4 paragraphe 2 de ce traité et, d'autre part, que cette réponse n'est pas de nature à garantir l'effectivité des objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des infractions et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme, composante de l'objectif de valeur constitutionnelle de protection de l'ordre public.

Par quatre nouveaux mémoires, enregistrés les 15 mars, 29 mars, 7 avril et 8 avril 2021, les associations requérantes persistent dans leurs conclusions. Elles demandent en outre au Conseil d'Etat d'enjoindre au Premier ministre de procéder à l'abrogation demandée sous astreinte de 50 000 euros par jour de retard et de mettre à la charge de l'Etat une somme de 31 415 euros au titre de l'article L. 761-1 du code de justice administrative.

3° Sous le n° 424717, par une requête, deux mémoires en réplique et trois nouveaux mémoires, enregistrés au secrétariat du contentieux du Conseil d'Etat les 5 octobre 2018 et les 11 janvier, 19 février, 5 mars, 19 mars et 7 avril 2021, la société Free Mobile demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur sa demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques ;

2°) d'enjoindre au Premier ministre d'abroger ces dispositions ou, à défaut, de statuer à nouveau sur sa demande dans un délai de quinze jours ;

3°) de mettre à la charge de l'Etat la somme de 10 000 euros au titre de l'article L. 761-1 du code de justice administrative.

La société soutient que les dispositions dont l'abrogation a été demandée sont illégales dès lors qu'elles ont été prises pour l'application de dispositions législatives qui portent une atteinte disproportionnée au droit au respect de la vie privée et familiale, au droit à la protection des données à caractère personnel et à la liberté d'expression, garantis par les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, et méconnaissent l'article 15, paragraphe 1, de la directive 2002/58/CE du parlement européen et du conseil du 12 juillet 2002 tel qu'interprété par la Cour de justice de l'Union européenne.

Par un mémoire en défense, enregistré le 22 janvier 2019, le ministre de l'économie et des finances conclut au rejet de la requête. Il soutient que le moyen invoqué n'est pas fondé.

Par un mémoire en défense et trois nouveaux mémoires, enregistrés les 21 janvier, 8 mars, 7 avril et 9 avril 2021, le Premier ministre conclut au rejet de la requête. Il soutient que le moyen invoqué n'est pas fondé et soulève les mêmes moyens en défense que sous le n° 393099.

4° Sous le n° 424718, par une requête, deux mémoires en réplique et trois nouveaux mémoires, enregistrés au secrétariat du contentieux du Conseil d'Etat les 5 octobre 2018 et les 11 janvier, 19 février, 5 mars, 19 mars et 7 avril 2021, la société Free demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur sa demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques ;

2°) d'enjoindre au Premier ministre d'abroger ces dispositions ou, à défaut, de statuer à nouveau sur sa demande dans un délai de quinze jours ;

3°) de mettre à la charge de l'Etat la somme de 10 000 euros au titre de l'article L. 761-1 du code de justice administrative.

La société soutient que les dispositions dont l'abrogation a été demandée sont illégales dès lors qu'elles ont été prises pour l'application de dispositions législatives qui portent une atteinte disproportionnée au droit au respect de la vie privée et familiale, au droit à la protection des données à caractère personnel et à la liberté d'expression, garantis par les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, et méconnaissent l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 tel qu'interprété par la Cour de justice de l'Union européenne.

Par un mémoire en défense, enregistré le 22 janvier 2019, le ministre de l'économie et des finances conclut au rejet de la requête. Il soutient que le moyen invoqué n'est pas fondé.

Par un mémoire en défense et trois nouveaux mémoires, enregistrés les 21 janvier, 8 mars, 7 avril et 9 avril 2021, le Premier ministre conclut au rejet de la requête. Il soutient que le moyen invoqué n'est pas fondé et soulève les mêmes moyens en défense que sous le n° 393099.

Vu les autres pièces des dossiers, y compris celles visées par les décisions du Conseil d'Etat du 26 juillet 2018 ;

Vu :
- la Constitution ;
- 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 de Budapest du 23 novembre 2001 sur la cybercriminalité ;
- le règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- le code des postes et des communications électroniques ;
- le code de procédure pénale ;
- le code de la sécurité intérieure, notamment son livre VIII ;

- la loi n° 2004-575 du 21 juin 2004 ;

- le décret n° 2011-219 du 25 février 2011 ;

- le décret n° 2015-1185 du 28 septembre 2015 ;

- le décret n° 2015-1639 du 11 décembre 2015 ;

- le décret n° 2016-67 du 29 janvier 2016 ;

- le décret n° 2020-1404 du 18 novembre 2020 ;

- l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014, Digital Rights Ireland Ltd (C-293/12 et C-594/12) ;

- l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016, 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) ;

- l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020, La Quadrature du net et autres (C-511/18, C-512/18, C520/18) ;

- l'arrêt de la Cour de justice de l'Union européenne du 2 mars 2021, H.K. / Prokuratuur (C-746/18) ;

- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Réda Wadjinny-Green, auditeur,

- les conclusions de M. Alexandre Lallet, rapporteur public ;

Vu la note en délibéré, enregistrée le 16 avril 20201, présentée sous les n[os] 393099, 394922, 397844 et 397851 par les associations French Data Network, La Quadrature du Net, la Fédération des fournisseurs d'accès à internet associatifs et Igwan.net.

Vu la note en délibéré, enregistrée le 16 avril 2021, présentée sous les n[os] 393099, 394922, 397844, 397851, 424717 et 424718 par le Premier ministre.

Considérant ce qui suit :

1. Les associations et sociétés requérantes contestent les dispositions réglementaires imposant aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus de conserver de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs ainsi que leurs données d'identité civile et certaines données relatives à leurs comptes et aux paiements qu'ils effectuent en ligne. Elles contestent également les dispositions réglementaires permettant aux services de renseignement de recueillir et d'opérer des traitements sur ces données. Sous le n° 393099, les associations French Data Network, La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du

décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. 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 n° 394922, du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement et, sous le n° 397851, du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. Sous le n° 397844, l'association Igwan.net demande l'annulation pour excès de pouvoir 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 même code. Sous les n^os 424717 et 424718, les sociétés Free Mobile et Free demandent l'annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques. Par ses décisions n° 393099 et n^os 394922, 394925, 397844, 397851 du 26 juillet 2018, le Conseil d'Etat, statuant au contentieux, a écarté les moyens invoqués devant lui autres que ceux tirés de la méconnaissance du droit de l'Union européenne et a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions préjudicielles dont il l'a saisie. Par un arrêt en date du 6 octobre 2020, rendu dans les affaires jointes C-511/18, C-512/18 et C-520/18, la Cour de justice s'est prononcée sur ces questions.

2. Les requêtes présentent à juger des questions communes. Il y a lieu de les joindre pour statuer par une seule décision.

I. Sur le cadre juridique des litiges :

En ce qui concerne les exigences inhérentes à la hiérarchie des normes :

3. En vertu de l'article 88-1 de la Constitution : « *La République participe à l'Union européenne constituée d'Etats qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007* ». Selon le paragraphe 3 de l'article 4 du traité sur l'Union européenne : « *En vertu du principe de coopération loyale, l'Union et les États membres se respectent et s'assistent mutuellement dans l'accomplissement des missions découlant des traités. / Les États membres prennent toute mesure générale ou particulière propre à assurer l'exécution des obligations découlant des traités ou résultant des actes des institutions de l'Union. / Les États membres facilitent l'accomplissement par l'Union de sa mission et s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union* ». La seconde phrase du paragraphe 1 de l'article 19 du même traité assigne à la Cour de justice de l'Union européenne la mission d'assurer « *le respect du droit dans l'interprétation et l'application des traités* ».

4. Le respect du droit de l'Union constitue une obligation tant en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne qu'en application de l'article 88-1 de la Constitution. Il emporte l'obligation de transposer les directives et d'adapter le droit interne aux règlements européens. En vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin

inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif.

5. Toutefois, tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne, dans les conditions mentionnées au point précédent, l'article 88-1 confirme la place de la Constitution au sommet de ce dernier. Il appartient au juge administratif, s'il y a lieu, de retenir de l'interprétation que la Cour de justice de l'Union européenne a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent. Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la Cour de justice de l'Union européenne, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige.

6. Il en résulte, d'une part, que, dans le cadre du contrôle de la légalité et de la constitutionnalité des actes réglementaires assurant directement la transposition d'une directive européenne ou l'adaptation du droit interne à un règlement et dont le contenu découle nécessairement des obligations prévues par la directive ou le règlement, il appartient au juge administratif, saisi d'un moyen tiré de la méconnaissance d'une disposition ou d'un principe de valeur constitutionnelle, de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué. Dans l'affirmative, il y a lieu pour le juge administratif, afin de s'assurer de la constitutionnalité de l'acte réglementaire contesté, de rechercher si la directive que cet acte transpose ou le règlement auquel cet acte adapte le droit interne est conforme à cette règle ou à ce principe général du droit de l'Union. Il lui revient, en l'absence de difficulté sérieuse, d'écarter le moyen invoqué, ou, dans le cas contraire, de saisir la Cour de justice de l'Union européenne d'une question préjudicielle, dans les conditions prévues par l'article 167 du traité sur le fonctionnement de l'Union européenne. En revanche, s'il n'existe pas de règle ou de principe général du droit de l'Union garantissant l'effectivité du respect de la disposition ou du principe constitutionnel invoqué, il revient au juge administratif d'examiner directement la constitutionnalité des dispositions réglementaires contestées.

7. D'autre part, lorsqu'il est saisi d'un recours contre un acte administratif relevant du champ d'application du droit de l'Union et qu'est invoqué devant lui le moyen tiré de ce que cet acte, ou les dispositions législatives qui en constituent la base légale ou pour l'application desquelles il a été pris, sont contraires à une directive ou un règlement européen, il appartient au juge administratif, après avoir saisi le cas échéant la Cour de justice d'une question préjudicielle portant sur l'interprétation ou la validité de la disposition du droit de l'Union invoquée, d'écarter ce moyen ou d'annuler l'acte attaqué, selon le cas. Toutefois, s'il est saisi par le défendeur d'un moyen, assorti des précisions nécessaires pour en apprécier le bien-fondé, tiré de ce qu'une règle de droit national, alors même qu'elle est contraire à la disposition du droit de l'Union européenne invoquée dans le litige, ne saurait être écartée sans priver de garanties effectives une exigence constitutionnelle, il appartient au juge administratif de rechercher s'il existe une règle ou un principe général du droit de l'Union européenne qui, eu égard à sa nature et à sa portée, tel qu'il est interprété en l'état actuel de la jurisprudence du juge de l'Union, garantit par son application l'effectivité de l'exigence constitutionnelle invoquée. Dans l'affirmative, il lui revient, en l'absence de difficulté sérieuse justifiant une question préjudicielle

à la Cour de justice, d'écarter cette argumentation avant de faire droit au moyen du requérant, le cas échéant. Si, à l'inverse, une telle disposition ou un tel principe général du droit de l'Union n'existe pas ou que la portée qui lui est reconnue dans l'ordre juridique européen n'est pas équivalente à celle que la Constitution garantit, il revient au juge administratif d'examiner si, en écartant la règle de droit national au motif de sa contrariété avec le droit de l'Union européenne, il priverait de garanties effectives l'exigence constitutionnelle dont le défendeur se prévaut et, le cas échéant, d'écarter le moyen dont le requérant l'a saisi.

8. En revanche, et contrairement à ce que soutient le Premier ministre, il n'appartient pas au juge administratif de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la Cour de justice elle-même, de la répartition des compétences entre l'Union européenne et les Etats membres. Il ne saurait ainsi exercer un contrôle sur la conformité au droit de l'Union des décisions de la Cour de justice et, notamment, priver de telles décisions de la force obligatoire dont elles sont revêtues, rappelée par l'article 91 de son règlement de procédure, au motif que celle-ci aurait excédé sa compétence en conférant à un principe ou à un acte du droit de l'Union une portée excédant le champ d'application prévu par les traités.

En ce qui concerne les exigences constitutionnelles invoquées en défense par l'Etat :

9. Il est soutenu en défense que les dispositions du droit national contestées au motif qu'elles seraient contraires au droit de l'Union européenne ne sauraient être écartées sans priver de garanties effectives les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme. Il ressort en effet de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789 que la garantie des droits de l'homme et du citoyen, sans laquelle une société n'a point de constitution selon l'article 16 de la même Déclaration, nécessite une force publique. La sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales constituent des objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée.

10. Selon le paragraphe 2 de l'article 4 du traité sur l'Union européenne, il appartient à l'Union, y compris à la Cour de justice de l'Union européenne, de respecter l'identité nationale des Etats membres, « *inhérente à leurs structures fondamentales politiques et constitutionnelles* », ainsi que « *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* », cette dernière restant « *de la seule responsabilité des Etats membres* ». Aux termes du paragraphe 1 de l'article 52 de la Charte des droits fondamentaux de l'Union européenne : « *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* ». Il ressort de la jurisprudence de la Cour de justice de l'Union européenne, d'une part, que les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et des

libertés d'autrui, sont au nombre des objectifs d'intérêt général reconnus par l'Union, comme tels susceptibles de justifier des limitations aux droits garantis par la Charte en vertu de son article 52, et, d'autre part, que si l'article 6 de la Charte, qui garantit le droit à la sûreté, ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer des infractions pénales, il découle de ses articles 3, 4 et 7, qui garantissent le droit au respect de l'intégrité de la personne, l'interdiction de la torture et des peines et traitements inhumains ou dégradants et le respect de la vie privée et familiale, des obligations positives à la charge de l'Etat, incluant la mise en place de règles permettant une lutte effective contre certaines infractions pénales. Toutefois, les exigences constitutionnelles mentionnées au point 9, qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.

En ce qui concerne l'office du juge dans le contentieux du refus d'abroger un acte réglementaire :

11. L'autorité compétente, saisie d'une demande tendant à l'abrogation d'un règlement illégal, est tenue d'y déférer, soit que, réserve faite des vices de forme et de procédure dont il serait entaché, ce règlement ait été illégal dès la date de sa signature, soit que l'illégalité résulte de circonstances de droit ou de fait postérieures à cette date.

12. L'effet utile de l'annulation pour excès de pouvoir du refus d'abroger un acte réglementaire illégal réside dans l'obligation, que le juge peut prescrire d'office en vertu des dispositions de l'article L. 911-1 du code de justice administrative, pour l'autorité compétente, de procéder à l'abrogation de cet acte afin que cessent les atteintes illégales que son maintien en vigueur porte à l'ordre juridique. Il s'ensuit que lorsqu'il est saisi de conclusions aux fins d'annulation du refus d'abroger un acte réglementaire, le juge de l'excès de pouvoir est conduit à apprécier la légalité de l'acte réglementaire dont l'abrogation a été demandée au regard des règles applicables à la date de sa décision.

En ce qui concerne les questions soulevées par les requêtes :

13. Les associations et sociétés requérantes contestent la conformité au droit de l'Union européenne de deux séries de dispositions. La première d'entre elles concerne l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, pris respectivement pour l'application de l'article L. 34-1 du même code et de l'article 6 de la loi du 21 juin 2004. Ces dispositions imposent aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de conserver, pour une durée d'un an, l'ensemble des données de trafic et de localisation de leurs utilisateurs, lesquelles ne couvrent pas le contenu des communications, les données relatives à leur identité civile, ainsi que certaines informations relatives à leurs comptes et, le cas échéant, aux paiements qu'ils effectuent en ligne pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et la sauvegarde de la sécurité nationale. La seconde série de dispositions concerne les décrets du 28 septembre 2015, du 11 décembre 2015 et du 29 janvier 2016, pris pour l'application du livre VIII de la partie législative du code de la sécurité intérieure relatif au renseignement. Sont en particulier en cause les techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4 de ce code. Il y a lieu d'analyser successivement aux II et III de la

présente décision la compatibilité au droit de l'Union européenne de chacune de ces séries de dispositions.

II. Sur la conservation générale et indifférenciée des données de connexion :

En ce qui concerne le cadre juridique national :

14. Le II de l'article L. 34-1 du code des postes et des communications électroniques fait obligation aux opérateurs de services de communications électroniques, notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, d'effacer ou de rendre anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI du même article. Les données relatives au trafic au sens de ces dispositions sont définies par le 18° de l'article L. 32 du même code comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ». Elles incluent les données d'identification des utilisateurs des réseaux de communications électroniques, les données relatives aux caractéristiques techniques des communications qu'ils ont effectuées à l'aide de tels réseaux et, enfin, les données de localisation, définies par le c) de l'article 2 de la directive 2002/58/CE du 12 juillet 2002 comme « *toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

15. Par exception à la règle fixée au II de l'article L. 34-1 du code des postes et des communications électroniques, les opérateurs sont autorisés par le IV du même article à conserver, d'une part, les catégories de données énumérées aux I à III de l'article R. 10-14 de ce code, pour les besoins de la facturation et du paiement des prestations de communications électroniques qu'ils fournissent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, soit un an à compter du jour du paiement en vertu de l'article L. 34-2 et, d'autre part, les données énumérées au IV de cet article R. 10-14, pour les besoins de la sécurité des réseaux et des installations, pour une durée n'excédant pas trois mois.

16. Par dérogation au principe d'anonymisation des données de connexion, le III du même article L. 34-1 prévoit la possibilité d'imposer aux opérateurs de communications électroniques la conservation des données relatives au trafic et à la localisation, pour une durée maximale d'un an, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. Il dispose ainsi que : « *III. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et*

la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs ». Le VI du même article précise que : « *VI. – Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. / Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. / La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. / Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article* ».

17. Le 2° de l'article L. 39-3 du code des postes et des communications électroniques punit d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents de ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

18. Le premier alinéa du II de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit par ailleurs que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

19. Pour les besoins du renseignement, l'article L. 851-1 du code de la sécurité intérieure, relatif aux accès administratifs aux données de connexion par les services de renseignement, prévoit que, dans les conditions prévues au chapitre I[er] du titre II du livre VIII de ce code, 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 et à l'article 6 de la loi du 21 juin 2004, 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. Selon l'article L. 811-3 du code de la sécurité intérieure, « *pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : / 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; / 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; / 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; / 4° La prévention du terrorisme ; / 5° La prévention : / a) Des atteintes à la forme républicaine des institutions ; / b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; / c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; / 6° La prévention de la criminalité et de la délinquance organisées ; / 7° La*

prévention de la prolifération des armes de destruction massive ». L'article L. 811-4 renvoie à un décret en Conseil d'Etat le soin de désigner les services, autres que les services spécialisés de renseignement, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du même livre VIII.

20. Il résulte de l'ensemble des dispositions mentionnées aux points précédents que le législateur a entendu imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs l'obligation de conserver de manière générale et indifférenciée les données de connexion pour les besoins, d'une part, de la recherche, de la constatation et de la poursuite des infractions, notamment pénales, et, d'autre part, des missions de défense et de promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement, dans les conditions et limites fixées par la loi et les dispositions réglementaires prises pour son application.

En ce qui concerne les dispositions réglementaires dont il est demandé l'abrogation :

21. L'article R. 10-13 du code des postes et des communications électroniques, dont le refus d'abrogation est contesté sous les n^os 393099, 424717 et 424718, énumère les données qui doivent être conservées, pour une durée d'un an à compter du jour de leur enregistrement, par les opérateurs de communications électroniques aux fins mentionnées au point précédent. Sont concernées par cette obligation : « a) Les informations permettant d'identifier l'utilisateur ; / b) Les données relatives aux équipements terminaux de communication utilisés ; / c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; / d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; / e) Les données permettant d'identifier le ou les destinataires de la communication ». Il prévoit également que, pour les activités de téléphonie, l'opérateur doit conserver les données relatives au trafic « et, en outre, celles permettant d'identifier l'origine et la localisation de la communication ».

22. Pour l'application des dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, l'article 1er du décret du 25 février 2011, dont le refus d'abrogation est contesté sous le n° 393099, prévoit que : « Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes : / 1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés : / a) L'identifiant de la connexion ; / b) L'identifiant attribué par ces personnes à l'abonné ; / c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ; / d) Les dates et heure de début et de fin de la connexion ; / e) Les caractéristiques de la ligne de l'abonné ; / 2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création : / a) L'identifiant de la connexion à l'origine de la communication ; / b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ; / c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ; / d) La nature de l'opération ; / e) Les date et heure de l'opération ; / f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ; / 3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte : / a) Au moment de la création du compte, l'identifiant de cette connexion ; / b) Les nom et prénom ou la raison sociale ; / c) Les adresses postales associées ; / d) Les pseudonymes utilisés ; / e) Les adresses de courrier électronique ou de compte associées ; / f) Les numéros de téléphone ; /

g) Les données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour ; / 4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement : / a) Le type de paiement utilisé ; / b) La référence du paiement ; / c) Le montant ; / d) La date et l'heure de la transaction ».

En ce qui concerne les exigences qui découlent du droit de l'Union européenne :

S'agissant des textes de droit dérivé applicables :

23. La directive 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* ». Aux termes de son article 5 : « *1. Les Etats 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* », tandis qu'en vertu de son article 6 : « 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* ». Toutefois, l'article 15 de la même directive prévoit que « *Les Etats 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'Etat – 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* ».

24. Il résulte des articles 1er et 2 de cette directive, tels qu'interprétés par la Cour de justice de l'Union européenne, que les dispositions précitées s'appliquent aux opérateurs de services de communications électroniques, c'est-à-dire aux services qui consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, tels que les services d'accès à internet. Les opérateurs mentionnés à l'article L. 34-1 du code des postes et des communications électroniques, notamment les fournisseurs d'accès à internet et les opérateurs de téléphonie, ainsi que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne au sens du paragraphe 1 du I de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, ce qui vise en particulier les fournisseurs d'accès à internet, relèvent du champ d'application de cette directive. Tel n'est pas le cas, en revanche, des « hébergeurs », c'est-à-dire des personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, mentionnées au paragraphe 2 du I du même article 6, dès lors que leurs services ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

25. L'article 23 du règlement du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (RGPD) prévoit que : « *1. Le droit de l'Union ou le droit de l'Etat 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 aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir : / 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* (…) ». Les hébergeurs mentionnés au point précédent constituent, au titre de cette activité, des responsables de traitement de données à caractère personnel, comme tels soumis aux dispositions de ce règlement.

26. Il ressort des dispositions citées aux points précédents que les Etats membres sont autorisés, pour des motifs tenant à la sauvegarde de la sécurité nationale, à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à prévoir une dérogation, d'une part, à l'obligation de confidentialité des données à caractère personnel et, d'autre part, à celle de confidentialité des données relatives au trafic y afférentes, qui découlent toutes deux de l'article 5, paragraphe 1, de la directive, ainsi qu'aux droits et obligations prévues aux articles 12 à 22 du RGPD.

S'agissant de la réponse apportée par la Cour de justice de l'Union européenne aux questions préjudicielles posées par le Conseil d'Etat :

27. Par son arrêt du 6 octobre 2020 La Quadrature du Net et autres (C-511/18, C-512/18, C-520/18), la Cour de justice de l'Union européenne a, en réponse aux questions que lui avait posées le Conseil d'Etat dans sa décision avant-dire droit du 26 juillet 2018, dit pour droit que : « *1) L'article 15, paragraphe 1, de 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 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, 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 des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives / - permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ; / - prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et / - permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services / dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

28. Si la Cour a également dit pour droit que « *l'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services* », elle a relevé, au point 211 de sa décision, qui constitue le soutien nécessaire de cette partie du dispositif, que : « *les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux*

première et deuxième questions dans l'affaire C-520/18 s'appliquent mutatis mutandis *à l'article 23 du règlement 2016/679* ». Il en ressort clairement que les conditions permettant de déroger aux droits et obligations prévus aux articles 12 à 22 du RGPD sur le fondement de l'article 23 du règlement et celles permettant de déroger à l'interdiction de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation sur le fondement de l'article 15, paragraphe 1 de la directive du 12 juillet 2002 sont identiques.

29. Il résulte de ce qui a été dit aux points 27 et 28 que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et l'article 23 du RGPD, tels qu'interprétés par la Cour de justice dans son arrêt du 6 octobre 2020, limitent la possibilité d'imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation des données de connexion de leurs utilisateurs. L'encadrement précisé par la Cour de justice diffère selon la nature des données en cause, les finalités poursuivies et le type de conservation.

30. En premier lieu, le droit de l'Union européenne s'oppose à ce que soit imposée aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP, y compris aux fins de lutte contre la criminalité grave. Toutefois, il est possible d'imposer aux opérateurs une conservation ciblée de ces données, en fonction de catégories de personnes, dont des éléments objectifs permettent d'établir que leurs données sont susceptibles de révéler un lien au moins indirect avec des actes de criminalité grave, de contribuer, d'une manière ou d'une autre, à la lutte contre cette criminalité ou de prévenir un risque grave pour la sécurité publique, d'une part, ou en fonction de zones géographiques caractérisées par un risque élevé de préparation ou de commission d'actes de criminalité grave, d'autre part.

31. En revanche et en deuxième lieu, le droit de l'Union européenne permet d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP aux seules fins de sauvegarde de la sécurité nationale lorsqu'un Etat est confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, sur injonction d'une autorité publique, soumise à un contrôle effectif d'une juridiction ou d'une autorité administrative indépendante, chargée notamment de vérifier la réalité de la menace, pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

32. En troisième lieu, le droit de l'Union européenne permet d'imposer aux opérateurs une « conservation rapide » des données de trafic et de localisation, c'est-à-dire une obligation à effet immédiat de conserver en l'état et pour une durée limitée au strict nécessaire certaines des données dont ils disposent, sous le contrôle d'un juge, lorsque ces données sont susceptibles de contribuer à l'élucidation d'une infraction grave ou à la prévention de menaces graves contre la sécurité publique. Ces données ne sont pas limitées aux personnes soupçonnées d'être les auteurs de l'infraction, mais peuvent être étendues à d'autres personnes pour les besoins de l'enquête, sur le fondement de critères objectifs.

33. En quatrième lieu, la conversation généralisée et indifférenciée des adresses IP peut être imposée aux fournisseurs d'accès à internet et aux hébergeurs, pour une période limitée au strict nécessaire, dès lors qu'elle peut constituer, comme le relève la Cour au point 154 de sa décision, le seul moyen d'investigation permettant l'identification d'une personne ayant commis une infraction en ligne. Toutefois, dès lors qu'une telle conservation emporte une

ingérence grave dans les droits fondamentaux des personnes concernées, elle ne saurait être justifiée qu'aux fins de lutte contre la criminalité grave, pour la prévention des menaces graves contre la sécurité publique et pour la sauvegarde de la sécurité nationale.

34. En dernier lieu, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs est possible, sans délai particulier, aux fins de prévention des menaces à la sécurité publique, de recherche, de détection et de poursuite des infractions pénales en général et de sauvegarde de la sécurité nationale. Ainsi que la Cour le relève au point 157 de sa décision, l'ingérence qu'emporte la conservation de telles données ne saurait, en principe, être qualifiée de grave dès lors que ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes.

En ce qui concerne la compatibilité avec le droit de l'Union européenne des dispositions en litige :

S'agissant de la conservation générale et indifférenciée des données relatives à l'identité civile, aux paiements, aux contrats et aux comptes de l'abonné :

35. Ainsi qu'il a été dit au point 34, les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques peuvent faire l'objet, sans limitation de durée, d'une conservation généralisée et indifférenciée pour les besoins de toute procédure pénale, de la prévention de toute menace contre la sécurité publique et de la sauvegarde de la sécurité nationale. Il suit de là que l'article R. 10-13 du code des postes et des communications électroniques et l'article 1[er] du décret du 25 février 2011, en tant qu'ils prévoient l'obligation pour les opérateurs de conserver de telles données, ne sont pas contraires au droit de l'Union européenne.

36. En outre, il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement aux 3° et 4° de l'article 1[er] du décret du 25 février 2011.

S'agissant de la conservation générale et indifférenciée des adresses IP :

37. Il résulte de l'arrêt de la Cour de justice précité que, dans la mesure où elles ne révèlent aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication, et où elles peuvent constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction, les adresses IP attribuées à la source d'une connexion peuvent faire l'objet d'une obligation de conservation généralisée et indifférenciée à des fins de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique, pour une période temporellement limitée au strict nécessaire.

38. Si la conservation généralisée et indifférenciée des adresses IP ne saurait être justifiée par les besoins de la lutte contre l'ensemble des infractions pénales, il ne résulte pas des énonciations de l'arrêt de la Cour de justice de l'Union européenne que le législateur serait tenu d'énumérer les infractions relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne. Le rattachement d'une infraction pénale à la criminalité grave a donc vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce. Une obligation de conservation généralisée et indifférenciée des adresses IP peut ainsi être imposée aux opérateurs, dès lors que les conditions d'accès à ces données par les services d'enquête sont fixées en fonction de la gravité des infractions susceptibles de le justifier, dans le respect du principe de proportionnalité, lequel fait partie des principes généraux du droit de l'Union européenne.

39. Les associations requérantes soutiennent que les dispositions attaquées relatives à la conservation des adresses IP méconnaissent le droit de l'Union européenne dès lors qu'elles ne circonscrivent pas cette conservation aux seules fins de lutte contre la criminalité grave. Or, aux termes de l'article préliminaire du code de procédure pénale : « *Au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction* ». Conformément au principe de proportionnalité consacré par cet article, l'obligation de conservation résultant du III de l'article L. 34-1 du code des postes et des communications électroniques et du II de l'article 6 de la loi du 21 juin 2004 n'est donc imposée aux opérateurs, sous le contrôle des juridictions compétentes, que pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales susceptibles de présenter un degré de gravité suffisant pour justifier l'ingérence dans les droits protégés par les articles 4, 7 et 11 de la Charte des droits fondamentaux de l'Union européenne. Seules de telles infractions pouvant légalement justifier l'accès des services d'enquêtes aux données conservées par les opérateurs, il s'ensuit que la conservation des adresses IP imposée de façon généralisée et indifférenciée aux opérateurs ne saurait être regardée comme méconnaissant les exigences de la directive du 12 juillet 2002.

40. En outre, il résulte du III de l'article R. 10-13 du code des postes et des communications électroniques et de l'article 3 du décret du 25 février 2011 que les adresses IP ne peuvent être conservées qu'un an. Il ne ressort pas des pièces du dossier que cette durée de conservation ne serait pas strictement nécessaire aux besoins de la lutte contre la criminalité grave et de la prévention des menaces graves pour la sécurité publique.

41. Il résulte de ce qui précède que l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, en tant qu'ils prévoient une obligation de conservation généralisée et indifférenciée des adresses IP, ne sont pas contraires au droit de l'Union européenne.

S'agissant de la conservation générale et indifférenciée des données de trafic et de localisation autres que les adresses IP :

42. Ainsi qu'il a été dit au point 31, la Cour a dit pour droit que la directive ne s'opposait pas à ce que des mesures législatives permettent, aux fins de sauvegarde de la sécurité nationale, d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de

trafic et des données de localisation, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, pour une durée limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. Il ressort en outre du point 135 de son arrêt du 6 octobre 2020 que la responsabilité des Etats membres en matière de sécurité nationale, au sens du droit de l'Union, correspond à l'intérêt primordial de protéger les fonctions essentielles de l'Etat et les intérêts fondamentaux de la société, et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'Etat en tant que tel, telles que notamment des activités de terrorisme.

Quant à la conservation générale et indifférenciée de ces données de connexion aux fins de sauvegarde de la sécurité nationale :

43. En premier lieu, les dispositions citées aux points 16, 18 et 19 imposent la conservation généralisée et indifférenciée, pour une durée d'un an, des données énumérées à l'article R. 10-13 du code des postes et des communications électroniques et à l'article 1er du décret du 25 février 2011 en vue de défendre et de promouvoir les intérêts fondamentaux de la Nation énumérés à l'article L. 811-3 du code de la sécurité intérieure, de même que pour les besoins de la recherche, de la constatation et de la poursuite d'infractions qui mettent en cause la sécurité nationale, notamment les atteintes aux intérêts fondamentaux de la Nation figurant au titre Ier du livre IV du code pénal et le terrorisme réprimé par les dispositions de son titre II. Dans cette mesure, cette obligation de conservation imposée aux opérateurs, mise en œuvre par des dispositions à caractère réglementaire susceptibles de faire l'objet d'un recours pour excès de pouvoir devant le juge administratif, assorti, le cas échéant, d'une demande de suspension de leurs effets sur le fondement de l'article L. 521-1 du code de justice administrative, ou d'un référé fondé sur l'article L. 521-2 du même code, est justifiée, dans son principe, par l'objectif de sauvegarde de la sécurité nationale.

44. En deuxième lieu, il ressort des pièces du dossier, notamment des mesures d'instruction diligentées par la dixième chambre de la section du contentieux, que la France est confrontée à une menace pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure cité au point 19 qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau « Urgence attentat » entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau « Sécurité renforcée – risque attentat » depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire. Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique. De nombreuses entreprises françaises, tant des grands groupes que des petites et moyennes entreprises, font ainsi l'objet d'actions malveillantes, visant leur savoir-faire et leur potentiel d'innovation, à travers des opérations d'espionnage industriel ou scientifique, de sabotage, d'atteintes à la réputation ou de débauchage d'experts. La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes. Ces menaces sont de nature à justifier l'obligation de conservation généralisée et indifférenciée des données de connexion listées à l'article R. 10-13 du code des postes et des

communications électroniques autres que les données relatives à l'identité civile et aux adresses IP. En outre, il ne ressort pas des pièces du dossier que la durée de conservation de ces données, fixée à un an, ne serait pas strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale.

45. En troisième lieu, toutefois, ni l'article L. 34-1 du code des postes et des communications électroniques, ni l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique ne prévoient un réexamen périodique, au regard des risques pour la sécurité nationale, de la nécessité de maintenir l'obligation faite aux personnes concernées de conserver les données de connexion. Les dispositions de ces articles, ainsi, par suite, que celles de l'article R. 10-13 du code des postes et des communications électroniques et du décret du 25 février 2011, en tant qu'elles ne subordonnent pas le maintien en vigueur de cette obligation au constat, à échéance régulière, qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible, pour la sécurité nationale sont, dans cette mesure, contraires au droit de l'Union européenne. Par ailleurs, le fait d'imposer aux pouvoirs publics un tel réexamen n'affecte pas, par lui-même, les exigences constitutionnelles mentionnées au point 9.

46. Il résulte de ce qui précède que, s'agissant de l'objectif de sauvegarde de la sécurité nationale, le refus d'abroger l'article R. 10-13 du code des postes et des communications électroniques et l'article 1[er] du décret du 25 février 2011 doit être annulé en tant seulement que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP. Il y a lieu d'enjoindre au Gouvernement de compléter ces dispositions dans un délai de six mois à compter de la présente décision. Dans la mesure où il résulte de la présente décision, ainsi qu'il a été dit au point 44, que la réalité et la gravité de la menace pesant sur la sécurité nationale justifient l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin, les opérateurs ne sauraient, avant l'expiration de ce délai, se soustraire à cette obligation et aux sanctions dont sa méconnaissance est assortie au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire.

Quant à la conservation générale et indifférenciée de ces données de connexion aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public :

47. Les dispositions mentionnées aux points 16 et 18 organisent également la conservation généralisée et indifférenciée des données de connexion pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales, ou de manquements à certaines législations particulières, ne mettant pas en jeu la sécurité nationale.

48. Ainsi qu'il a été rappelé aux points 30 à 34, le droit de l'Union européenne, tel qu'interprété par la Cour de justice, s'oppose à une obligation de conservation généralisée et indifférenciée des données de connexion, autres que celles d'identification des utilisateurs et les adresses IP, aux fins de lutte contre la criminalité et la prévention des menaces pour la sécurité publique, quel que soit le degré de gravité de cette criminalité ou de ces menaces.

49. Le Premier ministre soutient en défense que l'obligation pour le juge d'écarter les dispositions du droit national imposant une conservation généralisée et indifférenciée des données de connexion pour des finalités autres que de sauvegarde de la sécurité nationale priverait de garanties effectives les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, et de recherche des auteurs d'infractions pénales.

50. En premier lieu, il ressort des pièces du dossier, notamment des mesures d'instruction diligentées par la dixième chambre de la section du contentieux, ainsi que des échanges intervenus au cours de la séance orale d'instruction qui s'est tenue le 22 mars 2021, que l'obligation de conservation généralisée et indifférenciée des données de connexion pour une période d'un an, imposée aux opérateurs sur le fondement des dispositions mentionnées aux points 16, 18, 21 et 22, est une condition déterminante de succès des enquêtes conduites en vue de la recherche, de la constatation et de la poursuite des auteurs d'infractions à caractère criminel et délictuel. L'exploitation ultérieure de ces données, en particulier des données de localisation du détenteur d'un équipement terminal, est en effet, dans de très nombreuses hypothèses, l'unique moyen de retrouver leurs auteurs. Il ne ressort en outre pas des pièces du dossier que des méthodes alternatives puissent utilement s'y substituer. Par construction, les méthodes d'investigation traditionnelles, telles que les filatures et les surveillances, outre les aléas auxquelles elles sont confrontées, ne permettent pas d'apporter d'éléments sur des événements passés et sont inefficaces pour les infractions dématérialisées. Les méthodes d'investigation scientifique, telles que la recherche d'empreintes digitales et de traces génétiques, ne peuvent être efficaces que si des éléments matériels sont laissés par les auteurs d'infraction. A l'inverse, s'il existe des méthodes d'investigation complexes présentant une réelle efficacité pour l'élucidation des crimes et délits, comme la captation de données en temps réel, elles sont plus intrusives et plus attentatoires aux libertés. L'accès différé aux données de connexion revêt une importance d'autant plus cruciale que l'utilisation des moyens de communications électroniques, notamment cryptées, constitue un instrument qui facilite la commission de ces crimes et délits et rend plus difficile la recherche de leurs auteurs. Il permet, à l'inverse, de lever les soupçons pesant sur des personnes suspectées, à tort, d'y être impliquées.

51. En deuxième lieu, les articles 5, 6 et 9 de la directive 2002/58 ménagent, il est vrai, aux opérateurs la faculté de conserver certaines données pour les besoins de l'acheminement des communications et des opérations de facturation et de paiement des services rendus. Ces dispositions sont transposées au IV de l'article L. 34-1 et à l'article R. 10-14 du code des postes et des communications électroniques. Il résulte de ces dispositions, combinées avec l'article L. 34-2 du même code, que les données nécessaires aux opérations relatives à la facturation et au paiement des factures sont susceptibles d'être conservées jusqu'à l'expiration du délai de prescription des demandes en restitution du prix des prestations formées par les utilisateurs, fixé à un an à compter du jour du paiement, ou des demandes de paiement des prestations formulées par les opérateurs, également fixé à un an à compter de la date d'exigibilité des sommes. Toutefois, il ressort des pièces du dossier que seule une partie des données couvertes par l'article R. 10-13 est volontairement conservée par les opérateurs pour leurs besoins propres ou pour la sécurité des réseaux et installations au titre du seul article R. 10-14, et pour des durées moindres. En particulier, les données de connexion relatives aux appels entrants et celles relatives à la géolocalisation ne font que très rarement l'objet d'une conservation à ce titre de la part des opérateurs. De même, les données relatives aux appels sortants dans le cadre de forfaits illimités ne sont pas conservées dès lors qu'elle ne sont pas utiles à la facturation. Or le recueil de ces données contribue de façon déterminante à l'efficacité des enquêtes pénales.

52. En troisième lieu, il résulte de la jurisprudence de la Cour de justice que la directive ne s'oppose pas à une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable, en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

53. Il ressort cependant des pièces du dossier, notamment des éléments recueillis auprès de la Fédération française des télécoms, qu'une telle conservation ciblée se heurte à des obstacles techniques qui en compromettent manifestement la mise en œuvre. En ce qui concerne une conservation ciblée selon des critères géographiques, il apparaît que l'implantation des relais de téléphonie mobile et de leurs cellules est propre à chaque opérateur, que le mode de propagation des ondes radio émises par les relais de téléphonie mobile n'est pas compatible avec des limites géographiques prédéfinies et que l'information de localisation n'est pas systématiquement présente dans les données collectées. Les sociétés Free Mobile et Free indiquent, quant à elles, que les données de connexion stockées dans leur système d'information ne sont pas associées à une zone géographique particulière, qu'au surplus cette localisation est changeante dans le temps et qu'elles ne sont en mesure d'établir une corrélation entre la « cellule » radio à laquelle sont associées des données de connexion et la localisation géographique de cette cellule qu'au cas par cas, en réponse à une réquisition judiciaire. Quant à une conservation ciblée sur des personnes, la Fédération française des télécoms fait valoir qu'elle se heurterait au fait que les informations contenues dans les données de trafic ne permettent pas d'effectuer un tri selon des catégories de personnes. Les sociétés Free et Free Mobile précisent, pour leur part, que les personnes sont identifiées par des données – le numéro de téléphone, le numéro IMSI et le numéro IMEI – qui peuvent varier dans le temps et que ces données sont gérées de façon étanche pour répondre aux exigences du RGPD.

54. En outre, une conservation ciblée, à la supposer techniquement possible, présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas, y compris en cas de faits particulièrement graves, d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte. Ainsi, notamment pour les cas de primo-délinquants, mais également lorsque les auteurs d'infractions pénales ont recours à des téléphones dotés de cartes prépayées qu'ils n'utilisent que pour une durée limitée et qui, par construction, n'auraient pu être préalablement identifiés, les services d'enquête judiciaire ne pourraient pas accéder aux données de connexion indispensables à l'élucidation des affaires dont ils sont saisis. Par ailleurs, il est impossible de définir par avance des zones géographiques où, par nature, aucun acte de criminalité grave susceptible de justifier la conservation des données de connexion ne pourrait survenir. Une obligation de conservation des données de connexion limitée à certaines zones géographiques, à supposer même qu'elle soit techniquement envisageable, ferait ainsi obstacle à l'action des services d'enquête dans les autres parties du territoire national lorsque de telles infractions y seraient commises. Enfin, aucune présomption de dangerosité ne saurait être légalement retenue à l'encontre de personnes en fonction de leur lieu de résidence ou d'activité professionnelle pour justifier la conservation de leurs données de trafic et de localisation. Une différence de traitement instaurée sur ces fondements serait contraire au principe constitutionnel d'égalité devant la loi.

55. En quatrième lieu, la Cour de justice a admis, au regard de la directive 2002/58 et du RGPD, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un

contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données de trafic et des données de localisation dont disposent ces fournisseurs de services, au sens de l'article 16 de la convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001. Les stipulations de cette convention, à laquelle la France est partie, lui font obligation d'adopter les mesures nécessaires pour permettre à ses autorités, aux fins d'enquêtes et de procédures pénales et en vue d'assurer la collecte des preuves électroniques de toute infraction pénale, d'ordonner ou d'imposer d'une autre manière la conservation rapide de données de trafic, stockées au moyen d'un système informatique, et, en particulier pour obliger la personne qui les détient ou les contrôle à conserver et protéger l'intégrité de ces données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, le cas échéant renouvelable, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Selon la Cour de justice, une telle conservation rapide peut non seulement porter sur les données des personnes concrètement soupçonnées d'avoir projeté ou commis une infraction pénale ou une atteinte à la sécurité nationale, mais aussi sur les données d'autres personnes, pour autant qu'elles peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de cette infraction ou de cette atteinte à la sécurité nationale, telles que les données de la victime de celle-ci et de son entourage social ou professionnel, ou encore des données relatives à des zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction. Au point 164 de sa décision, la Cour précise ainsi que : « *Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient* ». Il s'ensuit que, lorsqu'est en cause une infraction suffisamment grave pour justifier l'ingérence dans la vie privée induite par la conservation des données de connexion, dans le respect du principe de proportionnalité rappelé aux points 38 et 39, l'autorité judiciaire peut, sans méconnaître ni la directive du 12 juillet 2002, ni le RGPD, enjoindre aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de sites internet de procéder à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.

56. La conservation rapide des données de connexion est ainsi de nature à faire obstacle à la disparition des informations nécessaires à la recherche, à la constatation et à la poursuite des auteurs d'infractions pénales à compter de la date et de l'heure à laquelle il est enjoint à un opérateur d'y procéder, à la suite de la commission d'une infraction ou du recueil d'éléments donnant à penser qu'une telle infraction est projetée, ainsi qu'à l'effacement ou à l'anonymisation des données relatives à des communications antérieures lorsqu'elles ont été conservées par les opérateurs. Cependant, sur ce dernier point, l'efficacité du dispositif est subordonnée à la condition que les données aient été effectivement conservées. A défaut, la

conservation rapide ne permet pas aux services d'enquête et à l'autorité judiciaire d'exploiter des données relatives aux communications effectuées avant qu'elle soit ordonnée.

57. Il résulte de ce qui précède que ni l'accès aux données de connexion conservées volontairement par les opérateurs, ni la possibilité de leur imposer une obligation de conservation ciblée, ni le recours à la technique de la conservation rapide ne permettent, par eux-mêmes, de garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales. Toutefois, d'une part, à la date de la présente décision, l'état des menaces pesant sur la sécurité nationale rappelées au point 44 justifie légalement que soit imposée aux opérateurs la conservation générale et indifférenciée des données de connexion. D'autre part, la conservation rapide des données susceptibles de contribuer à la recherche, la constatation et la poursuite des infractions pénales, dans le respect du principe de proportionnalité prévu par le code de procédure pénale conformément à ce qui a été rappelé au point 39, est possible dans les conditions prévues par la directive du 12 juillet 2002 et le RGPD, y compris, comme l'a jugé la Cour ainsi qu'il a été rappelé au point 55, lorsque cette conservation rapide porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. L'autorité judiciaire est donc en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie. Le même principe s'applique nécessairement aux autorités administratives indépendantes disposant d'un droit d'accès aux données de connexion en vertu de la loi en vue de lutter contre les manquements graves aux règles dont elles ont la charge d'assurer le respect. Dans ces conditions, le Premier ministre n'est pas fondé à soutenir qu'en l'état, la mise à l'écart des dispositions contestées du droit national, au motif qu'elles seraient contraires au droit de l'Union européenne, priverait de garanties effectives les objectifs de valeur constitutionnelle invoqués.

58. Il résulte de tout ce qui précède que le Gouvernement ne pouvait pas imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion, autres que les données mentionnées aux points 33, 34 et 36, relatives à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public sans méconnaître le droit de l'Union européenne. Il ressort du point précédent qu'à la date de la présente décision, et aussi longtemps que l'existence d'une menace grave sur la sécurité nationale justifie la conservation généralisée et indifférenciée des données de connexion, l'application du droit de l'Union européenne, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle invoqués par le Premier ministre en défense. Il y a dès lors lieu d'écarter les articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi du 21 juin 2004 en tant qu'ils poursuivent une finalité autre que celle de la sauvegarde de la sécurité nationale. Par suite, les associations requérantes sont fondées à soutenir que les dispositions du I et du II de l'article R. 10-13 du code des postes et des communications électroniques d'une part, et du 1° et du 2° de l'article 1[er] du décret du 25 février 2011 sont entachées d'illégalité dans cette mesure. C'est donc à tort que le Premier ministre a refusé d'en prononcer l'abrogation dans cette même mesure.

59. Il y a lieu de décider que le Premier ministre disposera d'un délai d'au plus six mois à compter de la notification de la présente décision pour limiter les finalités poursuivies par ces articles et adapter le cadre réglementaire relatif à la conservation des données de connexion. Il n'y a pas lieu, dans les circonstances de l'espèce, d'assortir cette injonction d'une astreinte.

III. Sur les traitements mis en œuvre par les services de renseignement sur les données de connexion :

60. Les associations requérantes contestent la conformité au droit de l'Union européenne de quatre techniques de renseignement. La première, définie par l'article L. 851-1 du code de la sécurité intérieure, permet aux services de renseignement d'accéder aux données de trafic et de localisation conservées par les opérateurs de communications électroniques, les fournisseurs d'accès à internet et les hébergeurs de contenu. La deuxième, définie à l'article L. 851-2 du code leur permet, pour les seuls besoins de prévention du terrorisme, de recueillir en temps réel ces données pour les personnes préalablement identifiées comme présentant une menace. La troisième, prévue par l'article L. 851-3 du code, permet la mise en place de traitements automatisés sur les données de connexion conservées par les opérateurs afin de détecter des connexions susceptibles de révéler une menace terroriste. Enfin, l'article L. 851-4 permet aux services de renseignement de recueillir en temps réel les données techniques relatives à la localisation des équipements terminaux de communications électroniques. Les associations requérantes soutiennent que ces dispositions méconnaissent le droit de l'Union européenne tel qu'interprété par l'arrêt de la Cour de justice du 6 octobre 2020. Il y a lieu d'apprécier, en premier lieu, l'opérance des moyens invoqués, en deuxième lieu, la conformité au droit de l'Union de chacune de ces méthodes de renseignement et, en troisième lieu, d'examiner les autres moyens invoqués tirés de ce que les garanties procédurales encadrant les dispositions législatives du livre VIII du code de la sécurité intérieure seraient insuffisantes au regard du droit de l'Union.

En ce qui concerne l'opérance du moyen tiré de ce que les dispositions législatives du code de la sécurité intérieure seraient incompatibles avec le droit de l'Union européenne :

61. Sous les n[os] 394922, 397844 et 397851, les associations requérantes soutiennent, par la voie de l'exception, que les articles L. 851-1 à L. 851-4 du code de la sécurité intérieure seraient incompatibles avec le droit de l'Union européenne.

62. La contrariété d'une disposition législative aux stipulations d'un traité international ou au droit de l'Union européenne 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.

63. Le décret du 28 septembre 2015 désigne, en application de l'article L. 811-2 du code de la sécurité intérieure, les services spécialisés de renseignement et prévoit les modalités d'application des articles L. 853-1 à L. 853-3 du code. Il suit de là que les associations requérantes ne sauraient utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 à L. 851-4 à l'appui de leurs conclusions dirigées contre ce décret, qui n'a pas été pris pour l'application de ces articles et dont ceux-ci ne constituent pas la base légale. La requête présentée sous le n° 394922 doit, par suite, être rejetée.

64. L'article 3 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, insère dans le code des articles R. 851-1 et R. 851-2 qui désignent les services autres que les services spécialisés de renseignement qui peuvent, pour des finalités qu'ils précisent, recourir aux techniques définies par les articles L. 851-1 et L. 851-4 du code. Les autres dispositions du décret ne sont pas prises pour l'application des articles L. 851-1 à L. 851-4 et ces articles n'en constituent pas la base légale. Il suit de là que l'association Igwan.net ne saurait utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 et L. 851-4 du code de la sécurité intérieure qu'à l'appui de ses conclusions dirigées contre les dispositions de l'article 3 du décret contesté en tant qu'il insère les articles R. 851-1 et R. 851-2 dans ce code. Ses conclusions dirigées contre les autres dispositions de ce décret ne peuvent, dès lors, qu'être rejetées.

65. L'article 1er du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement insère au code de la sécurité intérieure un article R. 823-1 qui précise le rôle du groupement interministériel de contrôle. Aux termes du 3° de cet article, ce service est chargé de : « Recueillir et conserver les informations ou documents mentionnés à l'article L. 851-1 dans les conditions fixées au chapitre Ier du titre V du présent livre ». Par ailleurs, l'article 2 du décret insère au même code un article R. 851-1-1, qui désigne les services autres que les services spécialisés de renseignement pouvant être autorisés à utiliser la technique mentionnée à l'article L. 851-2 du code de la sécurité intérieure au titre de la prévention du terrorisme, et des articles R. 851-5 à R. 851-10 qui précisent notamment les conditions d'application des articles L. 851-1 à L. 851-4. Les autres dispositions du décret ne sont pas prises pour l'application des articles L. 851-1 à L. 851-4 et ces articles n'en constituent pas la base légale. Il suit de là que les associations requérantes ne peuvent utilement contester, par la voie de l'exception, l'incompatibilité avec le droit de l'Union européenne des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure qu'à l'appui de leurs conclusions dirigées contre l'article 1er du décret attaqué en tant qu'il insère au code le 3° de l'article R. 823-1 et contre l'article 2 en tant qu'il insère au même code les articles R. 851-1-1 et R. 851-5 à R. 851-10. Leurs conclusions dirigées contre les autres dispositions de ce décret ne peuvent, dès lors, qu'être rejetées.

En ce qui concerne la conformité au droit de l'Union des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure :

S'agissant de l'accès administratif par les services de renseignement aux données de trafic et de localisation prévu par l'article L. 851-1 du code de la sécurité intérieure :

Quant au moyen tiré de ce que les dispositions attaquées organisent l'accès à des données conservées en méconnaissance du droit de l'Union :

66. Il ressort clairement des pièces du dossier qu'en 2015 et 2016, date à laquelle les décrets attaqués ont été adoptés, la France était confrontée à une menace grave, réelle et actuelle pour sa sécurité nationale, ainsi qu'en témoignent notamment l'attentat ayant visé « Charlie Hebdo » survenu le 7 janvier 2015 et la série d'attentats du 13 novembre 2015. Il s'ensuit que le livre VIII du code de la sécurité intérieure pouvait, ainsi qu'il a été dit précédemment, imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de sauvegarde de la sécurité nationale.

Quant aux finalités poursuivies par les services de renseignement :

67. Dans sa rédaction applicable au litige, 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* (…) ». En application de l'article L. 811-3 du même code : « *Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : / 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; / 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; / 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; / 4° La prévention du terrorisme ; / 5° La prévention : / a) Des atteintes à la forme républicaine des institutions ; / b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; / c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; / 6° La prévention de la criminalité et de la délinquance organisées ; / 7° La prévention de la prolifération des armes de destruction massive* ». Dès lors que ces finalités concourent à la défense des intérêts fondamentaux de la Nation, elles doivent être regardées comme relevant de la sauvegarde de la sécurité nationale au sens de l'article 15 de la directive du 12 juillet 2002.

Quant à l'existence d'un contrôle préalable :

68. Par son arrêt du 21 décembre 2016 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), la Cour de justice de l'Union européenne a dit pour droit que l'article 15 de la directive du 12 juillet 2002 devait : « *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* ». Le point 120 de cet arrêt précise que « *Aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* ». Si la Cour de justice n'a rappelé cette règle dans son arrêt du 6 octobre 2020 qu'à

propos du recueil en temps réel des données de connexion par les services de renseignement, elle a réitéré le principe du contrôle préalable de l'accès des autorités nationales aux données de connexion par une juridiction ou une autorité administrative indépendante dans son arrêt du 2 mars 2021, H.K. / Prokuratuur (C-746/18).

69. Il résulte de ce qui a été dit au point précédent que l'accès des services de renseignement aux données de trafic et de localisation conservées par les opérateurs de communications électroniques sur le fondement des articles L. 34-1 du code des postes et des communications électroniques et 6 de la loi du 21 juin 2004, pour les finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure, qui toutes relèvent de la sauvegarde de la sécurité nationale, est possible sans méconnaître les dispositions de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et de l'article 23 du RGPD, à condition que cet accès soit soumis, sauf en cas d'urgence dûment justifiée, à un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant et s'opère sur le fondement de critères objectifs et non discriminatoires.

70. D'une part, en vertu des articles L. 821-1 à L. 821-8 du code de la sécurité intérieure, la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code est soumise à l'autorisation préalable du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement, laquelle contrôle notamment le respect du principe de proportionnalité de l'atteinte à la vie privée qu'entrainent ces techniques, en vertu de l'article L. 801-1 du code. Cette autorisation est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes. L'autorisation de mise en œuvre de ces techniques est délivrée pour une durée maximale de quatre mois. Si, en cas d'urgence absolue et pour les seules finalités mentionnées aux points 1°, 4° et a) du 5° de l'article L. 811-3, le recours à ces techniques de renseignement peut être autorisé sans avis préalable de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre lui fait parvenir, dans un délai maximal de vingt-quatre heures, tous les éléments de motivation de la demande et ceux justifiant le caractère d'urgence absolue. Enfin, l'article L. 822-2 du code précise les délais dans lesquels les renseignements collectés doivent être détruits.

71. D'autre part, aux termes de l'article L. 833-4 du code de la sécurité intérieure : « *De sa propre initiative ou 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 commission 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. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre* ». Le Conseil d'Etat peut en outre être saisi, conformément à l'article L. 841-1 par : « *1° 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 ; / 2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8* ». Enfin, l'article L. 833-8 du code prévoit que : « *Le Conseil d'Etat peut être saisi d'un recours prévu au 2° de l'article L. 841-1 soit par le président de la commission 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, soit par au moins trois membres de la commission* ».

72. Il résulte de l'article L. 801-1 du code de la sécurité intérieure que l'autorité publique ne peut porter atteinte au respect de la vie privée, dans toutes ses composantes, notamment la protection des données à caractère personnel, que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. A ce titre, l'autorisation et la mise en œuvre sur le territoire national de la technique de renseignement prévue à l'article L. 851-1 de ce code ne peuvent être décidées que si elles procèdent d'une autorité ayant légalement compétence pour le faire, s'inscrivent dans les missions confiées aux services de renseignement, respectent la procédure d'autorisation et les règles de conservation par les services de renseignement définies au titre II du livre VIII de ce code, sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, et si les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.

73. La mise en œuvre de la technique de renseignement prévue à l'article L. 851-1 du code de la sécurité intérieure ne donne pas lieu au contrôle préalable par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant, dès lors que la Commission nationale de contrôle des techniques de renseignement n'émet qu'un avis simple ou des recommandations non contraignantes et que la saisine du Conseil d'Etat ne lui est ouverte, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, qu'après la délivrance de l'autorisation par le Premier ministre et, le cas échéant, sa mise en œuvre. En revanche, les exigences rappelées au point 68 sont respectées en cas d'urgence dûment justifiée, dans la mesure où, d'une part, le président de la commission ou trois de ses membres peuvent saisir le Conseil d'Etat à bref délai lorsque l'avis de cette commission ou, dans les cas d'urgence absolue mentionnés à l'article L. 821-5 du code de la sécurité intérieure, la recommandation de la commission tendant à l'interruption de la mise en œuvre de la technique de renseignement litigieuse, n'a pas été suivi et où, d'autre part, il appartient à la formation spécialisée dans le contentieux des techniques de renseignement de se prononcer dans les plus brefs délais.

74. La directive du 12 juillet 2002 et le RGPD, tels qu'interprétés par la Cour de justice, imposent la mise en place d'un contrôle juridictionnel ou assuré par une autorité administrative indépendante dotée d'un pouvoir contraignant préalablement à l'accès différé aux données de connexion par les services de renseignement, en-dehors des cas d'urgence dûment justifiée. Cette obligation impose d'écarter les dispositions législatives contestées dans la seule mesure où elles ne prévoient pas un tel contrôle préalable, ce qui n'est pas susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9. Il suit de là que le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement doit être annulé en tant qu'il permet l'accès en temps différé aux données de connexion par les services de renseignement, sans donner un caractère contraignant à l'avis de la Commission nationale de contrôle des techniques de renseignement, en-dehors des cas d'urgence dûment justifiée.

S'agissant de l'analyse automatisée des données de trafic et de localisation prévue à l'article L. 851-3 du code de la sécurité intérieure :

75. Aux termes de l'article L. 851-3 du code de la sécurité intérieure, dans sa rédaction applicable au litige : « I.- *Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, 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. / Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent. (...) II.- La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations (...) IV.- Lorsque les traitements mentionnés au I du présent article détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions prévues au chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes. Ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernées ».

76. Dans son arrêt du 6 octobre 2020 précité, la Cour a dit pour droit que : « *L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée (...) des données relatives au trafic et des données de localisation (...) lorsque / le recours à l'analyse automatisée est limité à des situations dans lesquelles un Etat membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues* ».

77. Il ne peut être recouru à l'analyse automatisée des données de trafic et de localisation prévue à l'article L. 851-3 du code de la sécurité intérieure que pour les seuls besoins de la prévention du terrorisme. La mise en œuvre de cette méthode n'est possible qu'après avis de la Commission nationale de contrôle des techniques de renseignement, laquelle est chargée, notamment, de vérifier qu'elle est mise en œuvre pour cette seule finalité et qu'elle repose sur des critères objectifs et non discriminatoires. A cette occasion, la Commission vérifie l'existence et l'actualité de la menace grave pour la sécurité nationale susceptible de justifier une telle mesure. Si l'avis de la Commission n'est pas doté d'un effet contraignant, le Conseil d'Etat peut être saisi d'un recours dans les conditions prévues à l'article L. 833-8 précité. Cette procédure respecte l'exigence qu'une telle méthode de renseignement puisse faire l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante. En revanche, si, en vertu du IV de l'article L. 851-3, lorsqu'une menace est détectée par un traitement automatisé, le Premier ministre peut autoriser l'identification des personnes concernées et le recueil des données y afférentes après un réexamen individuel, cette identification n'est pas subordonnée à un contrôle préalable exercé par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant. Il s'ensuit que le IV de l'article L. 851-3 du code de la sécurité intérieure méconnaît l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et l'article 23 du RGPD dans cette mesure. Il doit donc être écarté dans cette mesure seule, ce qui n'est pas

susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9, et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent la mise en œuvre de traitements automatisés sans prévoir un tel contrôle avant l'identification des personnes dont les données sont susceptibles de révéler une menace à caractère terroriste.

S'agissant du recueil en temps réel des données de trafic et de localisation prévu aux articles L. 851-2 et L. 851-4 du code de la sécurité intérieure :

78. Par son arrêt du 6 octobre 2020 précité, la Cour de justice de l'Union européenne a dit pour droit que : « *L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir (...) au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque (...) - le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais* ».

Quant à l'article L. 851-2 du code de la sécurité intérieure :

79. Dans sa rédaction applicable au litige, l'article L. 851-2 du code de la sécurité intérieure dispose que : « *I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée comme présentant une menace. / II.- Par dérogation à l'article L. 821-4, l'autorisation est délivrée pour une durée de deux mois, renouvelable dans les mêmes conditions de durée* ».

80. Il résulte de ce que la Cour a dit pour droit, et qui a été rappelé au point 78 de la présente décision, que le droit de l'Union européenne autorise le recueil en temps réel des données de trafic et de localisation lorsque celui-ci est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme. Il s'ensuit que la technique définie à l'article L. 851-2 du code de la sécurité intérieure, dans sa rédaction applicable à la date des décrets contestés, n'est pas contraire, dans son principe, aux dispositions de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 et de l'article 23 du RGPD telles qu'interprétées par la Cour de justice de l'Union européenne. En revanche, le recueil en temps réel des données de trafic et de localisation doit être soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dont la décision est dotée d'un effet contraignant. Or, d'une part, les avis que rend la Commission nationale de contrôle des techniques de renseignement ne sont pas contraignants et, d'autre part, l'article L. 833-8 du code de la sécurité intérieure ne prévoit pas de saisine

systématique du Conseil d'Etat lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission. Il s'ensuit que l'article L. 851-2 du code de la sécurité intérieure méconnaît les dispositions de la directive en tant qu'il ne prévoit pas de contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction. Il doit donc être écarté dans cette mesure seule et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent la mise en œuvre du recueil en temps réel des données de trafic et de localisation sans prévoir un tel contrôle. La mise à l'écart du droit national par le juge dans cette mesure n'est pas de nature à priver de garanties effectives les objectifs de valeur constitutionnelle cités au point 9.

Quant à l'article L. 851-4 du code de la sécurité intérieure :

81. Dans sa rédaction applicable au litige, l'article L. 851-4 du code de la sécurité intérieure dispose que : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre* ».

82. Il résulte de ce que la Cour a dit pour droit et qui a été rappelé au point 78 que l'article 15 de la directive du 12 juillet 2002 autorise le recueil en temps réel des données de localisation pour la prévention du terrorisme. Toutefois, il ne ressort pas de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020 que la directive interdirait le recours à cette méthode de renseignement pour la défense et la promotion des autres intérêts fondamentaux de la Nation définis à l'article L. 811-3 du code de la sécurité intérieure, dans le respect du principe de proportionnalité des atteintes à la vie privée rappelé à l'article L. 801-1 du code. Il s'ensuit que les associations requérantes ne sont pas fondées à soutenir que l'article L. 851-4 du code de la sécurité intérieure méconnaîtrait le droit de l'Union européenne en tant qu'il poursuivrait des finalités trop larges.

83. En revanche, et pour les mêmes motifs que ceux précisés au point 80 de la présente décision, l'article L. 851-4 du code de la sécurité intérieure méconnaît les dispositions de la directive en tant qu'il ne prévoit pas de contrôle préalable du recueil en temps réel des données de localisation par une autorité administrative indépendante dotée d'un pouvoir contraignant ou une juridiction. Il doit donc être écarté dans cette seule mesure, ce qui n'est pas susceptible de priver de garanties effectives les exigences constitutionnelles mentionnées au point 9, et les décrets attaqués doivent être annulés en tant seulement qu'ils permettent sa mise en œuvre sans prévoir un tel contrôle.

En ce qui concerne les moyens tirés de ce que les techniques du livre VIII du code de la sécurité intérieure seraient entourées de garanties procédurales insuffisantes :

S'agissant du moyen tiré de ce que les dispositions attaquées organisent l'accès aux données des personnes dont les communications sont soumises au secret professionnel, conservées en méconnaissance du droit de l'Union :

84. D'une part, il découle clairement de l'article 15 de la directive du 12 juillet 2002 que le droit de l'Union européenne ne s'oppose pas à ce que les données de connexion des personnes dont les communications sont soumises au secret professionnel fassent

l'objet d'une obligation de conservation en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. Il résulte de l'état de la menace rappelé aux points 44 et 66 que le pouvoir réglementaire pouvait légalement imposer aux opérateurs cités aux articles L. 34-1 du code des postes et des communications et 6 de la loi du 21 juin 2004 de conserver les données de trafic et de localisation de ces personnes.

85. D'autre part, les requérants soutiennent que les articles L. 851-1 à L. 851-4 du code de la sécurité intérieure méconnaissent le droit de l'Union européenne faute de prévoir des garanties légales pour le traitement des données de connexion des personnes dont les communications sont soumises au secret professionnel. Or, l'article L. 821-7 du code de la sécurité intérieure dispose, dans sa rédaction applicable au litige, que : « *Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession. Lorsqu'une telle demande concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière. L'article L. 821-5 n'est pas applicable. (...) Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ». Il s'ensuit que le moyen invoqué à ce titre manque en fait.

S'agissant des personnes susceptibles d'accéder aux données de trafic et de localisation :

86. Aux termes de l'article L. 811-4 du code de la sécurité intérieure : « *Un décret en Conseil d'Etat, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du présent livre dans les conditions prévues au même livre. Il précise, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation* ». Les associations requérantes soutiennent qu'en ne limitant pas le nombre de personnes pouvant accéder aux données de connexion et les exploiter, ces dispositions méconnaissent les droits au respect de la vie privée et familiale et à la protection des données à caractère personnel respectivement protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

87. Dans son arrêt du 8 avril 2014, Digital Rights Ireland Ltd (C-293/12 et C-594/12), la Cour de justice de l'Union européenne a dit pour droit que la directive 2006/24/CE du Parlement 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 était invalide, au motif notamment qu'elle ne prévoyait « *aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi* ».

88. En premier lieu, le décret du 11 décembre 2015 attaqué énumère limitativement, par technique de renseignement et par finalité poursuivie, les services autorisés à

recourir aux techniques du titre V du livre VIII de la partie législative du code de la sécurité intérieure. Le décret du 29 janvier 2016 également attaqué insère quant à lui au code de la sécurité intérieure un article R. 821-1 qui dispose que : « *Seuls peuvent mettre en œuvre les techniques de recueil de renseignement mentionnées au titre V du présent livre les agents individuellement désignés et habilités par le ministre ou, par délégation, par le directeur dont ils relèvent* ». De même, s'agissant plus précisément des méthodes de renseignement prévues par les articles L. 851-1, L. 851-2 et L. 851-4 du code, les articles R. 851-1, R. 851-1-1 et R. 851-2 du code issus des décrets attaqués prévoient également que seuls les agents individuellement désignés et habilités peuvent y recourir. Il résulte enfin du principe de proportionnalité, rappelé à l'article L. 801-1 du code, que le nombre des agents habilités ne saurait excéder celui nécessaire à l'exercice de ces activités.

89. En second lieu, il appartient au juge administratif, lorsqu'il est saisi d'un moyen en ce sens, de vérifier que l'accès aux données de connexion des personnes énumérées par les décrets pris pour l'application de l'article L. 811-4 et des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure est limité au strict nécessaire au regard des finalités poursuivies. Il s'ensuit que le moyen tiré de ce que ce décret méconnaîtrait les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne au motif qu'il ne limiterait pas le nombre de personnes pouvant accéder aux données de connexion et les exploiter doit être écarté.

S'agissant de l'information des personnes ayant fait l'objet d'une technique de renseignement :

90. Au point 190 de son arrêt du 6 octobre 2020 précité, la Cour de justice de l'Union européenne précise qu'il « *importe que les autorités nationales compétentes procédant au recueil en temps réel des données relatives au trafic et des données de localisation en informent les personnes concernées, dans le cadre des procédures nationales applicables, pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités* ».

91. L'article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose, dans sa version applicable au litige que : « *I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ; / 2° De la finalité poursuivie par le traitement auquel les données sont destinées (...) V. - Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement* ». Il résulte de ces dispositions que l'obligation d'information des personnes prévue par le I de cet article ne s'applique pas aux traitements mentionnés au V lorsqu'une telle limitation est nécessaire au respect des finalités poursuivies par ces traitements. En revanche, cette information est garantie dès lors qu'elle n'est plus susceptible de compromettre le respect des fins poursuivies par ces mêmes traitements. Ces dispositions doivent être regardées comme prévoyant, le cas échéant, l'information des personnes ayant fait l'objet d'un traitement de leurs données personnelles dans le cadre d'une des techniques de renseignement mentionnées aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre

les missions qui incombent aux services de renseignement, ainsi que l'exige la Cour de justice de l'Union européenne dans les motifs de son arrêt rappelés au point précédent. Il s'ensuit que les associations requérantes ne sont pas fondées à soutenir que les décrets attaqués méconnaîtraient le droit de l'Union, faute de prévoir une telle communication.

S'agissant des moyens dirigés contre des dispositions du code de la sécurité intérieure qui ne relèvent pas du champ de la directive du 12 juillet 2002 :

Quant à la durée de conservation des données recueillies sur le fondement de l'article L. 851-1 par les services de renseignement :

92. Les associations requérantes soutiennent que l'article L. 822-2 du code de la sécurité intérieure méconnaît la directive du 12 juillet 2002 en tant que la durée de conservation des données collectées par les services de renseignement sur le fondement de l'article L. 851-1 qu'il prévoit est excessive. L'article R. 851-6 inséré au code de la sécurité intérieure par le décret du 29 janvier 2016 attaqué dispose que : « II. - Le groupement interministériel de contrôle enregistre et conserve dans les mêmes conditions de durée que celles prévues à l'article L. 822-2 pour les renseignements collectés, dans un traitement automatisé qu'il met en œuvre, les demandes tendant au recueil mentionné à l'article L. 851-1 ainsi que les décisions du Premier ministre ou de ses délégués relatives à ces demandes ». Aux termes de l'article L. 822-2 du code de la sécurité intérieure dans sa rédaction applicable au litige : « *I. - Les renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement autorisée en application du chapitre Ier du présent titre sont détruits à l'issue d'une durée de : (...) 3° Quatre ans à compter de leur recueil pour les informations ou documents mentionnés à l'article L. 851-1. / Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de six ans à compter de leur recueil. / Dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, les renseignements collectés qui contiennent des éléments de cyberattaque ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au-delà des durées mentionnées au présent I* ».

93. En vertu de son article 1[er], paragraphe 3, la directive du 12 juillet 2002 « *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'Etat (y compris la prospérité économique de l'Etat lorsqu'il s'agit d'activités liées à la sûreté de l'Etat) ou aux activités de l'Etat dans des domaines relevant du droit pénal* ». Il en résulte clairement que les dispositions de l'article L. 822-2 du code de la sécurité intérieure ne relèvent pas du champ d'application de cette directive dès lors qu'elles fixent la durée pendant laquelle les services de renseignement peuvent conserver les données collectées sur le fondement de l'article L. 851-1 du même code, sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Ces dispositions ne sauraient donc 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 au moyen tiré de l'insuffisance du contrôle de l'exploitation des données collectées par les services de renseignement et de celui de la collecte et de l'exploitation des données transmises par des services étrangers :

94. Les associations requérantes soutiennent qu'en ne prévoyant pas de contrôle de l'exploitation des données collectées par les services de renseignement sur le fondement du livre VIII du code de la sécurité intérieure, d'une part, ni de contrôle de la conservation et de l'exploitation des données qui leur sont transmises par des services étrangers, d'autre part, les dispositions contestées méconnaissent le droit de l'Union européenne. Toutefois, il résulte clairement de l'article 1er, paragraphe 3 de la directive cité au point précédent que ni les règles relatives à l'exploitation par les services de renseignement des données collectées auprès des opérateurs ni celles relatives à la collecte et à l'exploitation par eux de données transmises par des services de renseignement étrangers ne régissent l'activité des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Il s'ensuit que ces règles ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et que le moyen soulevé ne peut être utilement invoqué à l'encontre des dispositions attaquées.

Quant aux moyens tirés de l'inconventionnalité de l'article L. 854-1 du code de la sécurité intérieure :

95. Les associations requérantes soutiennent à nouveau que l'article L. 854-1 du code de la sécurité intérieure méconnaît le droit de l'Union européenne. Toutefois, ainsi que l'a jugé le Conseil d'Etat, statuant au contentieux, au point 21 de sa décision n° 394922 et autres du 26 juillet 2018, 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.

En ce qui concerne les conséquences des illégalités affectant les décrets du 11 décembre 2015 et du 29 janvier 2016 :

96. Ainsi qu'il a été rappelé au point 66, la France était confrontée, à la date de publication des décrets attaqués, à une menace grave, réelle et actuelle pour sa sécurité nationale. Il ressort en outre des pièces du dossier que cette menace, dont les contours sont rappelés aux points 44 et 66, s'est maintenue à un niveau élevé entre cette date et celle de la présente décision. Il s'ensuit que, tout au long de cette période, le Gouvernement pouvait légalement imposer aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenu, la conservation généralisée et indifférenciée des données de trafic et de localisation aux fins de sauvegarde de la sécurité nationale.

97. Comme précisé aux points 74, 77, 80 et 83 de la présente décision, les articles L. 851-1, L. 851-2, L. 851-4 et le IV de l'article L. 851-3 méconnaissent le droit de l'Union européenne, faute pour la Commission nationale de contrôle des techniques de renseignement de disposer d'un pouvoir d'avis conforme. L'annulation des décrets attaqués en tant qu'ils permettent l'application de ces dispositions sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée, ne saurait toutefois avoir pour conséquence d'entacher d'illégalité, pour le passé, l'usage par les services de renseignement des techniques prévues par

ces articles que dans les hypothèses où le Premier ministre les aurait mises en œuvre, en dehors des cas d'urgence dûment justifiée, malgré un avis défavorable de la commission. Or, il ressort des rapports publics de la commission que l'avis rendu par celle-ci préalablement à la mise en œuvre de ces techniques de renseignement, bien qu'étant dépourvu d'effet contraignant, a été, dans les faits, systématiquement suivi par le Premier ministre. Il suit de là que l'annulation rétroactive des décrets attaqués, qui n'impliquerait par elle-même la suppression d'aucune donnée recueillie par les services de renseignement sur leur fondement, n'emporterait pas de conséquences manifestement excessives pas plus qu'elle ne priverait de garanties effectives les exigences constitutionnelles mentionnées au point 9.

98. Par ailleurs, l'annulation des décrets attaqués, compte tenu de sa portée, implique seulement, dans l'attente de l'intervention des textes nécessaires à la mise en conformité des dispositions du droit national avec le droit de l'Union européenne, qu'en cas d'avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre ne pourra légalement autoriser la mise en œuvre des techniques de renseignement mentionnées aux articles L. 851-1, L. 851-2, L. 851-4 et au IV de l'article L. 851-3 avant l'intervention de la décision du Conseil d'Etat, qu'il appartiendra alors à la commission de saisir en application de l'article L. 833-8 du même code. Dans ces conditions, il n'y a pas lieu de différer dans le temps les effets de l'annulation ainsi prononcée.

IV. Sur les conclusions tendant à l'application des dispositions de l'article L. 761-1 du code de justice administrative :

99. Il y a lieu de mettre à la charge de l'Etat la somme de 3 000 euros à verser à chacune des associations requérantes ainsi que la somme de 1 500 euros à verser aux sociétés Free Mobile et Free au titre de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : Sont annulées les décisions du Premier ministre refusant d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, en tant que ces dispositions réglementaires, d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP à la sauvegarde de la sécurité nationale et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

Article 2 : Il est enjoint au Premier ministre de procéder à cette abrogation dans un délai de six mois à compter de la présente décision.

Article 3 : Les décrets du 11 décembre 2015 et du 29 janvier 2016 sont annulés en tant seulement qu'ils permettent la mise en œuvre des dispositions des articles L. 851-1, L. 851-2, L. 851-4 et

du IV de l'article L. 851-3 du code de la sécurité intérieure sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiée.

Article 4 : La requête n° 394922 est rejetée.

Article 5 : L'Etat versera la somme de 3 000 euros à l'association La Quadrature du Net, 3 000 euros à l'association French Data Network, 3 000 euros à la Fédération des fournisseurs d'accès à internet associatifs, 3 000 euros à l'association Igwan.net, 1 500 euros à la société Free Mobile et 1 500 euros à la société Free au titre de l'article L. 761-1 du code de justice administrative.

Article 6 : Le surplus des conclusions des requêtes est rejeté.

Article 7 : La présente décision sera notifiée aux associations La Quadrature du Net, French Data Network, Igwan.net, à la Fédération des fournisseurs d'accès à internet associatifs, à la société Free Mobile, à la société Free, au Premier ministre, au ministre de l'économie, des finances et de la relance, à la ministre des armées, au ministre de l'intérieur, au garde des sceaux, ministre de la justice, à Privacy International et au Center for Democracy and Technology.

Copie en sera adressée à la Fédération française des télécoms.