Décision n° 2021 – 976/977 QPC

Article L. 34-11 paragraphes II et III du code des postes et télécommunications électroniques

Conservation des données de connexion pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales

Dossier documentaire

Source : services du Conseil constitutionnel - 2021

Sommaire

I. Contexte de la disposition contestée 5

II. Constitutionnalité de la disposition contestée 83

Table des matières

I. Contexte de la disposition contestée 5

A. Dispositions contestées 5

Code des postes et des télécommunications électroniques 5

- Article L. 34-1 5

B. Évolution des dispositions contestées 6

1. Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne 6

- Article 29 6

2. Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle 7

- Article 10 7
- Version consolidée 8

3. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers 9

- Article 5 9
- Version consolidée 9

4. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet 10

- Article 14 10
- Version consolidée 10

5. Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques 11

- Article 7 11
- Version consolidée 11

6. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale 12

- Article 24 12
- Version consolidée 13

7. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement 14

- Article 17 14
- Version consolidée de l'article 34-1 15

C. Autres dispositions 17

1. Code des postes et des télécommunications électroniques 17

- Article L. 32 17
- Article L. 39-3 22
- Article R. 10-13 [Version en vigueur au moment du litige] 22
- Article R. 10-13 [Version en vigueur] 22
- Article L. 450-3-3 23

2. Code de commerce 24

- Article L. 450-3-3 24

3. Code des douanes 25

- Article 65 quinquies 25

4. Code monétaire et financier 26

- Article L. 621-10-2 26

5. Code de procédure pénale 27

- Article 60-1 27
- Article 60-2 27

- Article 77-1-1 28
- Article 77-1-2 28
6. Livre des procédures fiscales 29
- Article L. 96 G 29
7. Code de la sécurité intérieure 29
- Article L. 851-1 29
- Article L. 851-2 30
8. Code du travail 30
- Article L. 8113-5-2 30
9. 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) 31
- Article 15 31

D. Application des dispositions contestées et d'autres dispositions 32
1. Jurisprudence 32
a. Jurisprudence communautaire 32
- CJUE, (grande chambre) du 8 avril 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.,* aff. C 293/12 et C-594/12. 32
- CJUE, (grande chambre) du 21 décembre 2016, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a, aff. C-203/15 et C-698/15 35
- CJUE, (grande chambre) du 2 octobre 2018, *Ministerio Fiscal,* aff. C-207/16 39
- CJUE, (grande chambre) du 6 octobre 2020, *La Quadrature du Net e.a. contre Premier ministre e.a.,* aff. C 511 /18 41
- CJUE, (grande chambre) du 2 mars 2021, *Prokuratuur,* aff. C-746/18 47
b. Jurisprudence administrative 51
- Conseil d'Etat, 10ème - 9ème chambres réunies, 26 juillet 2018, n° 394922 51
- Conseil d'Etat, Assemblée, 21 avril 2021, n°393099 57
c. Jurisprudence judiciaire 80
- Cour de cassation, 1er avril 2020, n° 19-80908 80

II. Constitutionnalité de la disposition contestée 83

A. Normes de référence 83
1. Déclaration des droits de l'homme et du citoyen de 1789 83
- Article 2 83
2. Constitution du 4 octobre 1958 83
- Article 34 83

B. Jurisprudence du Conseil constitutionnel sur le droit au respect de la vie privée 83
1. Sur le contrôle des fichiers et le traitement des données à caractère personnel 83
- Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle 83
- Décision n° 2003-467 DC du 13 mars 2003 - Loi pour la sécurité intérieure 84
- Décision n° 2011-625 DC du 10 mars 2011 - Loi d'orientation et de programmation pour la performance de la sécurité intérieure 86
- Décision n° 2012-652 DC du 22 mars 2012 - Loi relative à la protection de l'identité 88
- Décision n° 2013-684 DC du 29 décembre 2013 - Loi de finances rectificative pour 2013 88
- Décision n° 2014-690 DC du 13 mars 2014 - Loi relative à la consommation 89
- Décision n° 2016-591 QPC du 21 octobre 2016 - Mme Helen S. [Registre public des trusts] 90
- Décision n° 2016-745 DC du 26 janvier 2017 - Loi relative à l'égalité et à la citoyenneté 90
- Décision n° 2017-752 DC du 8 septembre 2017 - Loi pour la confiance dans la vie politique 91

- Décision n° 2017-637 QPC du 16 juin 2017 - Association nationale des supporters [Refus d'accès à une enceinte sportive et fichier d'exclusion] 91
- Décision n° 2017-670 QPC du 27 octobre 2017 - M. Mikhail P. [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires] 92
- Décision n° 2018-765 DC du 12 juin 2018 - Loi relative à la protection des données personnelles 93
- Décision n° 2019-796 DC du 27 décembre 2019 - Loi de finances pour 2020 94
- Décision n° 2019-797 QPC du 26 juillet 2019 - Unicef France et autres [Création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés] 97
- Décision n° 2020-800 DC du 11 mai 2020 - Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions 97
- Décision n° 2021-819 DC du 31 mai 2021 - Loi relative à la gestion de la sortie de crise sanitaire 99
- Décision n° 2021-952 QPC du 3 décembre 2021 - M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire] 101

2. Sur le contrôle en matière d'accès aux données de connexion 101

- Décision n° 2001-457 DC du 27 décembre 2001 - Loi de finances rectificative pour 2001 101
- Décision n° 2015-478 QPC du 24 juillet 2015 - Association French Data Network et autres [Accès administratif aux données de connexion] 102
- Décision n° 2015-715 DC du 5 août 2015 - Loi pour la croissance, l'activité et l'égalité des chances économiques 103
- Décision n° 2017-646/647 QPC du 21 juillet 2017 - M. Alexis K. et autre [Droit de communication aux enquêteurs de l'AMF des données de connexion] 103
- Décision n° 2018-764 QPC du 15 février 2019 - M. Paulo M. [Droit de communication aux agents des douanes des données de connexion] 104
- Décision n° 2019-789 QPC du 14 juin 2019 - Mme Hanen S. [Droit de communication des organismes de sécurité sociale] 104
- Décision n° 2020-841 QPC du 20 mai 2020 - La Quadrature du Net et autres [Droit de communication à la Hadopi] 105
- Décision n° 2021-952 QPC du 3 décembre 2021 - M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire] 106

I. Contexte de la disposition contestée

A. Dispositions contestées

Code des postes et des télécommunications électroniques

LIVRE II : Les communications électroniques

TITRE Ier : Dispositions générales

Chapitre II : Régime juridique.

Section 3 : Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques.

- **Article L. 34-1**

Version en vigueur du 20 décembre 2013 au 31 juillet 2021

Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

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.

IV. – Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. – Sans préjudice des dispositions du III et du IV et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la

communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

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.

B. Évolution des dispositions contestées

1. Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne

- **Article 29**

I. - Après l'article L. 32-3 du code des postes et télécommunications, sont insérés deux articles L. 32-3-1 et L. 32-3-2 ainsi rédigés :

« Art. L. 32-3-1. - I. - Les opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des II, III et IV.

« II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, 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 IV, 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.

« III. - Pour les besoins de la facturation et du paiement des prestations de télécommunications, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être également contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le IV, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

« Les opérateurs peuvent en outre réaliser un traitement de ces données en vue de commercialiser leurs propres services de télécommunications, si les usagers y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'usager et l'opérateur.

« IV. - Les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.

« 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 no 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.

(…)

2. Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle[1]

- **Article 10**

I. - La section 3 du chapitre II du titre Ier du livre II du même code est intitulée : « Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques ». Elle comprend les articles L. 32-3-1, L. 32-3-2, L. 32-5, L. 32-6 et L. 33-4-1 qui deviennent respectivement les articles L. 34-1, L. 34-2, L. 34-3, L. 34-4 et L. 34-5.

II. - L'article L. 34-1 du même code est ainsi modifié :

1° Le I est ainsi rédigé :

« I. - Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V. » ;

2° Au II et au III, les mots : « dans les limites fixées par le IV, » sont remplacés par les mots : « dans les limites fixées par le V, » ;

3° Le dernier alinéa du III est ainsi rédigé :

« Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux. » ;

4° Le IV devient le V ;

5° Après le III, il est rétabli un IV ainsi rédigé :

« IV. - Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation. » ;

6° Le premier alinéa du V est ainsi rédigé :

« Les données conservées et traitées dans les conditions définies aux II, III et IV 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. »

(…)

[1] Décision n° 2004-497 DC du 1er juillet 2004 - Loi relative aux communications électroniques et aux services de communication audiovisuelle

- **Version consolidée**

I. - ~~Les opérateurs de télécommunications, et notamment ceux mentionnés à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des II, III et IV.~~

Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V.

II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, 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 IV~~ **dans les limites fixées par le V**, 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.

III. - Pour les besoins de la facturation et du paiement des prestations de télécommunications, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être également contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, ~~dans les limites fixées par le IV~~ **dans les limites fixées par le V**, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

~~Les opérateurs peuvent en outre réaliser un traitement de ces données en vue de commercialiser leurs propres services de télécommunications, si les usagers y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'usager et l'opérateur.~~

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

IV. - Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

~~IV. - Les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.~~

Les données conservées et traitées dans les conditions définies aux II, III et IV 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 no 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.

3. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers2

- **Article 5**

Le I de l'article L. 34-1 du code des postes et des communications électroniques est complété par un alinéa ainsi rédigé :

« Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »

- **Version consolidée**

I. - ~~Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V~~.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, 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 V, 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.

III. - Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le V, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

IV. - Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

---

[2] Décision n° 2005-532 DC du 19 janvier 2006 - Loi relative à la lutte contre le terrorisme portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

V. - Les données conservées et traitées dans les conditions définies aux II, III et IV 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.

4. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet3

- **Article 14**

A la première phrase du II de l'article L. 34-1 du code des postes et des communications électroniques, après les mots : « infractions pénales», sont insérés les mots : « ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle » et après les mots : « l'autorité judiciaire », sont insérés les mots : « ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ».

- **Version consolidée**

I - Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II. - 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**, 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 d'informations, 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 V, 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.

III. - Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le V, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

IV. - Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la

[3] Décision n° 2009-580 DC du 10 juin 2009 – Loi favorisant la diffusion et la protection de la création sur internet

communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

V. - Les données conservées et traitées dans les conditions définies aux II, III et IV 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.

5. Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques

- **Article 7**

L'article L. 34-1 du même code est ainsi modifié :

1° Les I, II, III, IV et V deviennent respectivement II, III, IV, V et VI ;

2° Il est inséré au début de l'article un I ainsi rédigé :

« I. — Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification. » ;

3° Au premier alinéa du I devenu II, les mots : « des II, III, IV et V » sont remplacés par les mots : « des III, IV, V et VI » ;

4° Le II devenu III est ainsi modifié :

Au premier alinéa, la référence au : « V » est remplacée par la référence au : « VI » ;

5° Le II est complété par un second alinéa ainsi rédigé :

« Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes. » ;

6° Au III devenu IV, la référence au : « V » est remplacée par la référence au : « VI » ;

7° Au IV devenu V, les références : « du II et du III » sont remplacées par les références : « du III et du IV » ;

8° Au V devenu VI, les références : « aux II, III et IV » sont remplacées par les références : « aux III, IV et V

- **Version consolidée**

I. - Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

~~I~~ **II.-**Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

~~II~~. **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, 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 d'informations, 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 ~~V~~ **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.

~~III~~. **IV**-Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le ~~V~~ **VI**, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

~~IV~~. **V**-Sans préjudice des dispositions ~~du II et du III~~ **du III et du IV** et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

~~V~~. **VI**-Les données conservées et traitées dans les conditions définies ~~aux II, III et IV~~ **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.

6. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

- **Article 24**

(…)

II. — La première phrase du III de l'article L. 34-1 du code des postes et des communications électroniques est ainsi modifiée :

1° Après la référence : « article L. 336-3 du code de la propriété intellectuelle », sont insérés les mots : « 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 » ;

2° Après la référence : « article L. 331-12 du code de la propriété intellectuelle », sont insérés les mots : « ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense. »

- **Version consolidée**

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

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.

IV. – Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. – Sans préjudice des dispositions du III et du IV et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

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.

7. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement

- **Article 17**

I.-L'article L. 34-1 du code des postes et des communications électroniques est ainsi modifié :

1° A la fin du premier alinéa du II, les mots : « anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI » sont remplacés par les mots : « anonymes, sous réserve des II bis à VI, les données relatives aux communications électroniques » ;

2° Après le même II, il est inséré un II bis ainsi rédigé :

« II bis.-Les opérateurs de communications électroniques sont tenus de conserver :

« 1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

« 2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

« 3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux. » ;

3° Le III est ainsi rédigé :

« III.-Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'Etat.

« L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III. » ;

4° Après le même III, il est inséré un III bis ainsi rédigé :

« III bis.-Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données. » ;

5° A la première phrase du V, les mots : « et sous réserve des nécessités des enquêtes judiciaires » sont supprimés ;

6° Le VI est ainsi modifié :

a) Au premier alinéa, les références : « III, IV et V » sont remplacées par les références : « II bis à V » ;

b) Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II bis et III ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. »

(…)

- **Version consolidée de l'article 34-1**

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent ~~anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.~~ **anonymes, sous réserve des II bis à VI, les données relatives aux communications électroniques**

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II bis.-Les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

~~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.~~

III.-Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'Etat.

L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III.

III bis. Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données.

IV. – Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, 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, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le VI, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

V. – Sans préjudice des dispositions du III et du IV et ~~sous réserve des nécessités des enquêtes judiciaires~~, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

VI. – Les données conservées et traitées dans les conditions définies aux ~~III, IV et V~~ **II bis à 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.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II bis et III ainsi que les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.

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.

C. Autres dispositions

1. Code des postes et des télécommunications électroniques

LIVRE II : Les communications électroniques

TITRE Ier : Dispositions générales

Chapitre Ier : Définitions et principes.

- **Article L. 32**

1° Communications électroniques.

On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques.

2° Réseau de communications électroniques.

On entend par réseau de communications électroniques toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage.

Sont notamment considérés comme des réseaux de communications électroniques : les réseaux satellitaires, les réseaux terrestres, les systèmes utilisant le réseau électrique pour autant qu'ils servent à l'acheminement de communications électroniques et les réseaux assurant la diffusion ou utilisés pour la distribution de services de communication audiovisuelle.

2° bis Réseau de communications électroniques à très haut débit.

On entend par réseau de communications électroniques à très haut débit, un réseau de communications électroniques pouvant fournir des services d'accès à une vitesse supérieure ou égale à 30 Mbit/ s.

3° Réseau à très haute capacité.

On entend par réseau à très haute capacité, soit un réseau de communications électroniques qui est entièrement composé d'éléments de fibre optique au moins jusqu'au point de distribution au lieu de desserte, soit un réseau de communications électroniques qui est capable d'offrir, dans des conditions d'heures de pointe habituelles, une performance du réseau comparable en termes de débit descendant et ascendant, de résilience, de paramètres liés aux erreurs, de latence et de gigue.

4° Réseau ouvert au public.

On entend par réseau ouvert au public tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique.

4° bis Points de terminaison d'un réseau.

On entend par points de terminaison d'un réseau les points physiques par lesquels les utilisateurs accèdent à un réseau de communications électroniques ouvert au public et qui sont, dans le cas de réseaux utilisant la commutation et l'acheminement, identifiés par une adresse réseau spécifique, qui peut être rattachée au numéro ou au nom d'un utilisateur final. Ces points de raccordement font partie du réseau.

4° ter Boucle locale.

On entend par boucle locale l'installation qui relie le point de terminaison du réseau dans les locaux de l'abonné au répartiteur principal ou à toute autre installation équivalente d'un réseau de communications électroniques fixe ouvert au public.

5° Réseau indépendant.

On entend par réseau indépendant un réseau de communications électroniques réservé à l'usage d'une ou plusieurs personnes constituant un groupe fermé d'utilisateurs, en vue d'échanger des communications internes au sein de ce groupe.

6° Services de communications électroniques.

On entend par services de communications électroniques, les services fournis via des réseaux de communications électroniques qui comprennent au moins l'un des types de services suivants :

-un service d'accès à Internet ;

-un service de communications interpersonnelles ;

-un service consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion.

Ne sont pas visés les services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus.

6° bis Service de communications interpersonnelles.

On entend par service de communications interpersonnelles, un service qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires.

Ne sont pas visés les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service.

6° ter Service de communications interpersonnelles fondé sur la numérotation.

On entend par service de communications interpersonnelles fondé sur la numérotation, un service de communications interpersonnelles qui établit une connexion à un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation téléphonique ou qui permet la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation.

6° quater Service de communications interpersonnelles non fondé sur la numérotation.

On entend par service de communications interpersonnelles non fondé sur la numérotation, un service de communications interpersonnelles qui n'établit pas de connexion à un numéro ou des numéros figurant dans le plan national ou international de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans un plan national ou international de numérotation.

7° Service de communications vocales.

On entend par service de communications vocales, un service de communications électroniques accessible au public permettant d'émettre et de recevoir, directement ou indirectement, des appels nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros du plan national ou international de numérotation téléphonique.

8° Accès.

On entend par accès toute mise à disposition de moyens, matériels ou logiciels, ou de services, en vue de permettre au bénéficiaire de fournir des services de communications électroniques. Ne sont pas visés par le présent code les systèmes d'accès sous condition et les systèmes techniques permettant la réception de services de communication audiovisuelle, définis et réglementés par la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

9° Interconnexion.

On entend par interconnexion la liaison physique et logique des réseaux ouverts au public exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou bien d'accéder aux services fournis par un autre opérateur. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de réseaux ouverts au public.

10° Equipement terminal.

On entend par équipement terminal :

a) Tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de communications électroniques pour transmettre, traiter ou recevoir des informations ; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique ; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public ;

b) Les équipements de stations terrestres de satellites.

10° bis Systèmes d'exploitation.

On entend par systèmes d'exploitation les logiciels contrôlant les fonctions de base du matériel et les ressources logicielles d'un équipement terminal, permettant d'y exécuter des applications et aux utilisateurs d'en faire usage.

10° ter Fournisseur de systèmes d'exploitation.

On entend par fournisseur de système d'exploitation toute personne qui, à titre professionnel, édite ou adapte le système d'exploitation d'équipements terminaux ou qui édite ou adapte tout autre logiciel contrôlant l'accès aux fonctionnalités desdits équipements.

11° Réseau, installation ou équipement radioélectrique.

Un réseau, une installation ou un équipement sont qualifiés de radioélectriques lorsqu'ils utilisent intentionnellement des fréquences radioélectriques, en émission ou en réception, pour la propagation des ondes en espace libre, à des fins de radiocommunication ou de radiorepérage, y compris les équipements permettant de recevoir des services de radio ou de télévision.

Sont également considérés comme des équipements radioélectriques ceux qui doivent être complétés d'un accessoire tel qu'une antenne, pour émettre ou recevoir intentionnellement des fréquences radioélectriques à des fins de radiocommunication ou de radiorepérage.

Au nombre des réseaux radioélectriques figurent, notamment, les réseaux utilisant les capacités de satellites.

11° bis Centres de données.

On entend par centres de données les installations accueillant des équipements de stockage de données numériques.

12° Exigences essentielles.

On entend par " exigences essentielles " les exigences nécessaires pour garantir la préservation de l'intérêt général s'attachant :

– à la protection de la santé, de la sécurité des personnes et des animaux domestiques ainsi que des biens, dans des conditions fixées par décret en Conseil d'Etat ;

– au maintien d'un niveau adéquat de compatibilité électromagnétique entre équipements et installations de communications électroniques, dans des conditions fixées par décret en Conseil d'Etat ;

– à une utilisation efficace des fréquences radioélectriques par les équipements et à une contribution à l'utilisation optimisée de ces dernières en évitant des brouillages préjudiciables pour les tiers.

Les exigences essentielles comportent également, pour les classes et les catégories d'équipements prévues par décret en Conseil d'Etat, les exigences nécessaires à :

– la protection des réseaux, notamment des échanges d'informations de commande et de gestion qui y sont associés ;

– l'interopérabilité des services et celle des équipements radioélectriques ;

– la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés ;

– la compatibilité des équipements radioélectriques avec des accessoires, y compris des chargeurs universels, et avec des dispositifs empêchant la fraude, assurant l'accès aux services d'urgence, facilitant leur utilisation par les personnes handicapées ou garantissant qu'un logiciel ne peut être installé sur un équipement radioélectrique que lorsque la conformité de la combinaison de l'équipement radioélectrique avec le logiciel est avérée.

Aux fins du présent article, on entend par " interopérabilité des équipements radioélectriques " l'aptitude de ceux-ci à fonctionner, d'une part, avec le réseau et, d'autre part, avec les autres équipements radioélectriques.

13° Numéro géographique.

On entend par numéro géographique tout numéro du plan national de numérotation téléphonique dont la structure contient une indication géographique utilisée pour acheminer les appels vers le point de terminaison du réseau correspondant.

14° Numéro non géographique.

On entend par numéro non géographique tout numéro du plan national de numérotation téléphonique qui n'est pas un numéro géographique.

15° Opérateur.

On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.

15° bis Utilisateur final.

On entend par utilisateur final, un utilisateur qui ne fournit pas de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public.

16° Système satellitaire.

On entend par système satellitaire tout ensemble de stations terriennes et spatiales ayant pour objet d'assurer des radiocommunications spatiales et comportant un ou plusieurs satellites artificiels de la Terre.

17° Itinérance locale.

On entend par prestation d'itinérance locale celle qui est fournie par un opérateur de radiocommunications mobiles à un autre opérateur de radiocommunications mobiles en vue de permettre, sur une zone qui n'est couverte, à l'origine, par aucun opérateur de radiocommunications mobiles, l'accueil, sur le réseau du premier, des clients du second.

17° bis Itinérance ultramarine.

On entend par prestation d'itinérance ultramarine celle qui est fournie par un opérateur de radiocommunications mobiles sur le territoire de la France métropolitaine, d'un département d'outre-mer, de Mayotte, de Saint-Barthélemy, de Saint-Martin ou de Saint-Pierre-et-Miquelon à un autre opérateur de radiocommunications mobiles fournissant des services de communications mobiles sur réseau public terrestre dans un autre de ces territoires, en vue de permettre l'utilisation du réseau du premier, dit " opérateur du réseau visité " , par les clients du second, dit " opérateur du réseau d'origine " , pour émettre ou recevoir des communications à destination de l'un de ces territoires ou d'un Etat membre de l'Union européenne.

17° ter Partage d'un réseau radioélectrique ouvert au public.

On entend par partage d'un réseau radioélectrique ouvert au public l'utilisation d'éléments d'un réseau d'accès radioélectrique au bénéfice d'opérateurs de communications électroniques titulaires d'une autorisation d'utilisation de fréquences radioélectriques. Il comprend notamment les prestations d'itinérance ou de mutualisation de réseaux radioélectriques ouverts au public.

18° Données relatives au trafic.

On entend par données relatives au trafic toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation.

19° Ressources associées.

On entend par ressources associées, les services associés, les infrastructures physiques et les autres ressources associées à un réseau de communications électroniques ou à un service de communications électroniques, qui concourent ou peuvent concourir à la fourniture de services via ce réseau ou ce service. Sont notamment considérés comme des ressources associées les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, regards de visite, armoires et boîtiers.

20° Services associés.

On entend par services associés les services associés à un réseau ou à un service de communications électroniques et qui concourent ou peuvent concourir à la fourniture de services via ce réseau ou ce service. Sont notamment considérés comme des services associés les services de conversion du numéro d'appel, les systèmes d'accès conditionnel, les guides électroniques de programmes, ainsi que les services relatifs à l'identification, à la localisation et à la disponibilité de l'utilisateur.

21° Gestionnaire d'infrastructure d'accueil.

On entend par gestionnaire d'infrastructure d'accueil toute personne privée ou publique qui met à disposition ou exploite une infrastructure :

– permettant l'exploitation d'un réseau ouvert au public au sens du 3° ou d'un réseau destiné à fournir un service dans le domaine de la production, du transport ou de la distribution d'électricité, y compris pour l'éclairage public, de gaz ou de chaleur, d'eau y compris d'évacuation ou de traitement des eaux usées ; ou

– destinée à fournir des services de transport, y compris les voies ferrées, les routes, les ports et les aéroports.

22° Infrastructure d'accueil.

On entend par infrastructure d'accueil tout élément d'un réseau destiné à accueillir des éléments d'un réseau sans devenir lui-même un élément actif du réseau, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux, châteaux d'eau. Les câbles, y compris la fibre noire, ainsi que les éléments de réseaux utilisés pour la fourniture des eaux destinées à la consommation humaine ne sont pas des infrastructures d'accueil au sens du présent article.

22° bis Gestionnaire d'infrastructure d'accueil des points d'accès sans fil à portée limitée.

On entend par gestionnaire d'infrastructure d'accueil des point d'accès sans fil à portée limitée, toute personne privée ou publique qui met à disposition ou exploite une infrastructure d'accueil des points d'accès sans fil à portée limitée.

22° ter Infrastructure d'accueil des points d'accès sans fil à portée limitée.

On entend par infrastructure d'accueil des points d'accès sans fil à portée limitée, toute infrastructure physique contrôlée par l'Etat, les collectivités territoriales ou leurs groupements, techniquement adaptée pour héberger des points d'accès sans fil à portée limitée ou qui est nécessaire pour connecter de tels points d'accès à un réseau de collecte, y compris le mobilier urbain. Peuvent notamment être considérés comme une infrastructure d'accueil les poteaux d'éclairage, les panneaux et feux de signalisation, les panneaux d'affichage, les arrêts d'autobus et de tramway, les stations de métro.

22° quater Point d'accès sans fil à portée limitée.

On entend par point d'accès sans fil à portée limitée, un équipement d'accès sans fil au réseau à faible puissance, de taille réduite et de portée limitée, utilisant le spectre radioélectrique qui peut être équipé d'une ou plusieurs antennes à faible impact visuel et qui permet l'accès sans fil des utilisateurs aux réseaux de communications électroniques. Leurs caractéristiques physiques et techniques sont précisées par le règlement d'exécution (UE) 2020/1070 de la Commission du 20 juillet 2020 précisant les caractéristiques des points d'accès sans fil à portée limitée en application de l'article 57, paragraphe 2, de la directive (UE) 2018/1972 du Parlement européen et du Conseil établissant le code des communications électroniques européen.

23° Fournisseur de services de communication au public en ligne.

On entend par fournisseur de services de communication au public en ligne toute personne assurant la mise à disposition de contenus, services ou applications relevant de la communication au public en ligne, au sens du IV de l'article 1er de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Sont notamment considérées comme des fournisseurs de services de communication au public en ligne les personnes qui éditent un service de communication au public en ligne, mentionnées au deuxième alinéa du II de l'article 6 de la même loi, ou celles qui assurent le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature mentionnées au 2 du I du même article 6.

24° Réseau local hertzien ou RLAN.

On entend par réseau local hertzien, un système d'accès sans fil à faible puissance, de portée limitée, présentant un faible risque de brouillage avec d'autres systèmes similaires déployés à proximité immédiate par d'autres utilisateurs et utilisant, sur une base non exclusive, du spectre radioélectrique harmonisé.

25° Spectre radioélectrique harmonisé.

On entend par spectre radioélectrique harmonisé, un spectre radioélectrique dont les conditions harmonisées quant à sa disponibilité et son utilisation efficace ont été établies par la voie de mesures techniques d'application adoptées conformément à l'article 4 de la décision n° 676/2002/ CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne.

26° Utilisation partagée du spectre radioélectrique.

On entend par utilisation partagée du spectre radioélectrique, l'accès par deux utilisateurs ou plus aux mêmes bandes du spectre radioélectrique dans le cadre d'un dispositif de partage défini.

27° Ressources de numérotation.

On entend par ressources de numérotation les préfixes, numéros, blocs de numéros et codes utilisés pour l'acheminement des communications électroniques du plan national ou international de numérotation téléphonique qui ne relèvent pas du système de l'adressage de l'internet.

28° Communications d'urgence.

On entend par communications d'urgence, les communications effectuées au moyen de services de communications interpersonnelles, entre un utilisateur final et le centre de réception des communications d'urgence, dont le but est de demander et de recevoir des secours d'urgence de la part des services d'urgence.

29° Informations relatives à la localisation de l'appelant.

On entend par les informations relatives à la localisation de l'appelant, les données traitées qui proviennent de l'infrastructure de réseau ou de l'appareil mobile et qui indiquent la position géographique de l'équipement terminal mobile d'un utilisateur final et, dans un réseau fixe public, les données relatives à l'adresse physique du point de terminaison du réseau.

30° Marchés transnationaux.

On entend par marchés transnationaux, les marchés qui couvrent l'Union européenne ou une partie importante de celle-ci s'étendant sur plus d'un Etat membre.

31° Groupe pour la politique en matière de spectre radioélectrique.

On entend par Groupe pour la politique en matière de spectre radioélectrique, le groupe consultatif chargé d'assister et de conseiller la Commission européenne sur des questions liées à la politique du spectre radioélectrique.

32° Système automatisé d'appels et d'envois de messages.

On entend par système automatisé d'appels et d'envois de messages les systèmes émettant des appels ou des messages de manière automatique vers plusieurs utilisateurs finals conformément aux instructions établies pour ce système.

33° Opérateur de centre de données.

On entend par opérateur de centre de données toute personne assurant la mise à la disposition des tiers d'infrastructures et d'équipements hébergés dans des centres de données.

Chapitre V : Dispositions pénales.

- **Article L. 39-3**

Version en vigueur depuis le 10 juillet 2004

Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 () JORF 10 juillet 2004

I. – Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents :

1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise.

Partie réglementaire - Décrets en Conseil d'Etat

LIVRE II : Les communications électroniques

TITRE Ier : Dispositions générales

Chapitre II : Régime juridique.

Section 3 : Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques.

- **Article R. 10-13 [Version en vigueur au moment du litige]**

Version en vigueur du 01 avril 2012 au 21 octobre 2021

Modifié par Décret n°2012-436 du 30 mars 2012 - art. 7

I. – En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

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.

II. – Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. – La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

- **Article R. 10-13 [Version en vigueur]**

Modifié par Décret n°2021-1361 du 20 octobre 2021 - art. 3

I.-Les informations relatives à l'identité civile de l'utilisateur, au sens du 1° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° Les nom et prénom, la date et le lieu de naissance pour une personne physique ou la raison sociale, ainsi que les nom, prénom, date et lieu de naissance de la personne agissant en son nom, lorsque le compte est ouvert au nom d'une personne morale ;

2° La ou les adresses postales associées ;

3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ;

4° Le ou les numéros de téléphone.

II.-Les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° L'identifiant utilisé ;

2° Le ou les pseudonymes utilisés ;

3° Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour.

III.-Les informations relatives au paiement mentionnées au 2° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, pour chaque opération de paiement, lorsque la souscription du contrat ou la création du compte est payante, sont :

1° Le type de paiement utilisé ;

2° La référence du paiement ;

3° Le montant ;

4° La date, l'heure et le lieu en cas de transaction physique.

IV.-Les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, mentionnées au 3° du II bis de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver, sont :

1° L'adresse IP attribuée à la source de la connexion et le port associé ;

2° Le numéro d'identifiant de l'utilisateur ;

3° Le numéro d'identification du terminal ;

4° Le numéro de téléphone à l'origine de la communication.

V.-Les données de trafic et de localisation mentionnées au III de l'article L. 34-1, que les opérateurs de communications électroniques sont tenus de conserver sur injonction du Premier ministre, sont :

1° Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

2° Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

3° Les données techniques permettant d'identifier le ou les destinataires de la communication, mentionnées aux 1° à 4° du IV du présent article ;

4° Pour les opérations effectuées à l'aide de téléphones mobiles, les données permettant d'identifier la localisation de la communication.

VI. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

- **Article L. 450-3-3**

Version en vigueur depuis le 24 mai 2019

Création LOI n°2019-486 du 22 mai 2019 - art. 212

I.-Par dérogation aux deux derniers alinéas de l'article L. 450-3, pour la recherche et la constatation des infractions et manquements prévus au titre II du présent livre, l'accès aux données conservées et traitées par les opérateurs de télécommunication, dans les conditions et sous les limites prévues à l'article L. 34-1 du code des postes et des communications électroniques, et par les prestataires mentionnés 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 est réalisé dans les conditions définies au présent article.

II.-L'accès aux données mentionnées au I du présent article par les agents mentionnés à l'article L. 450-1 fait l'objet d'une demande d'autorisation préalable du rapporteur général de l'Autorité de la concurrence ou de l'autorité

administrative chargée de la concurrence et de la consommation auprès d'un contrôleur des demandes de données de connexion.

Le contrôleur des demandes de données de connexion est alternativement un membre du Conseil d'Etat, en activité ou honoraire, élu par l'assemblée générale du Conseil d'Etat, et un magistrat de la Cour de cassation, en activité ou honoraire, élu par l'assemblée générale de ladite Cour. Son suppléant, issu de l'autre juridiction, est désigné selon les mêmes modalités. Le contrôleur des demandes de données de connexion et son suppléant sont élus pour une durée de quatre ans non renouvelable.

Il ne peut être mis fin aux fonctions du contrôleur des demandes de données de connexion que sur sa demande ou en cas d'empêchement constaté, selon le cas, par le vice-président du Conseil d'Etat ou par le premier président de la Cour de cassation ou le procureur général près ladite Cour, sur saisine du ministre chargé de l'économie.

Le contrôleur des demandes de données de connexion ne peut recevoir ni solliciter aucune instruction de l'autorité de la concurrence, de l'autorité administrative chargée de la concurrence et de la consommation, ni d'aucune autre autorité dans l'exercice de sa mission.

La demande d'autorisation mentionne les éléments recueillis par les agents mentionnés à l'article L. 450-1 laissant présumer l'existence d'une infraction ou d'un manquement mentionnés au titre II du présent livre et justifiant l'accès aux données de connexion pour les besoins de l'enquête.

Les agents mentionnés à l'article L. 450-1 utilisent les données de connexion communiquées dans les conditions du présent article exclusivement dans le cadre de l'enquête pour laquelle ils ont reçu l'autorisation d'y accéder.

L'autorisation est versée au dossier d'enquête.

Ces données de connexion sont détruites à l'expiration d'un délai de six mois à compter d'une décision devenue définitive de l'Autorité de la concurrence, de l'autorité administrative chargée de la concurrence et de la consommation ou de la juridiction judiciaire ou administrative.

Les données de connexion relatives à des faits ne faisant pas l'objet de poursuites sont détruites à l'expiration d'un délai d'un mois à compter de la décision du rapporteur général de l'Autorité de la concurrence ou de l'autorité administrative mentionnée au I de l'article L. 470-2 ou de la juridiction judiciaire ou administrative, sans préjudice de leur transmission au procureur de la République en application de l'article 40 du code de procédure pénale.

Les modalités d'application du présent article sont précisées par décret en Conseil d'Etat.

2. Code de commerce

LIVRE IV : De la liberté des prix et de la concurrence.

TITRE V : Des pouvoirs d'enquête.

- **Article L. 450-3-3**

Version en vigueur depuis le 24 mai 2019

Création LOI n°2019-486 du 22 mai 2019 - art. 212

I.-Par dérogation aux deux derniers alinéas de l'article L. 450-3, pour la recherche et la constatation des infractions et manquements prévus au titre II du présent livre, l'accès aux données conservées et traitées par les opérateurs de télécommunication, dans les conditions et sous les limites prévues à l'article L. 34-1 du code des postes et des communications électroniques, et par les prestataires mentionnés 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 est réalisé dans les conditions définies au présent article.

II.-L'accès aux données mentionnées au I du présent article par les agents mentionnés à l'article L. 450-1 fait l'objet d'une demande d'autorisation préalable du rapporteur général de l'Autorité de la concurrence ou de l'autorité administrative chargée de la concurrence et de la consommation auprès d'un contrôleur des demandes de données de connexion.

Le contrôleur des demandes de données de connexion est alternativement un membre du Conseil d'Etat, en activité ou honoraire, élu par l'assemblée générale du Conseil d'Etat, et un magistrat de la Cour de cassation, en activité ou honoraire, élu par l'assemblée générale de ladite Cour. Son suppléant, issu de l'autre juridiction, est désigné selon les mêmes modalités. Le contrôleur des demandes de données de connexion et son suppléant sont élus pour une durée de quatre ans non renouvelable.

Il ne peut être mis fin aux fonctions du contrôleur des demandes de données de connexion que sur sa demande ou en cas d'empêchement constaté, selon le cas, par le vice-président du Conseil d'Etat ou par le premier président de la Cour de cassation ou le procureur général près ladite Cour, sur saisine du ministre chargé de l'économie.

Le contrôleur des demandes de données de connexion ne peut recevoir ni solliciter aucune instruction de l'autorité de la concurrence, de l'autorité administrative chargée de la concurrence et de la consommation, ni d'aucune autre autorité dans l'exercice de sa mission.

La demande d'autorisation mentionne les éléments recueillis par les agents mentionnés à l'article L. 450-1 laissant présumer l'existence d'une infraction ou d'un manquement mentionnés au titre II du présent livre et justifiant l'accès aux données de connexion pour les besoins de l'enquête.

Les agents mentionnés à l'article L. 450-1 utilisent les données de connexion communiquées dans les conditions du présent article exclusivement dans le cadre de l'enquête pour laquelle ils ont reçu l'autorisation d'y accéder.

L'autorisation est versée au dossier d'enquête.

Ces données de connexion sont détruites à l'expiration d'un délai de six mois à compter d'une décision devenue définitive de l'Autorité de la concurrence, de l'autorité administrative chargée de la concurrence et de la consommation ou de la juridiction judiciaire ou administrative.

Les données de connexion relatives à des faits ne faisant pas l'objet de poursuites sont détruites à l'expiration d'un délai d'un mois à compter de la décision du rapporteur général de l'Autorité de la concurrence ou de l'autorité administrative mentionnée au I de l'article L. 470-2 ou de la juridiction judiciaire ou administrative, sans préjudice de leur transmission au procureur de la République en application de l'article 40 du code de procédure pénale.

Les modalités d'application du présent article sont précisées par décret en Conseil d'Etat.

3. Code des douanes

Titre II : Organisation et fonctionnement du service des douanes

Chapitre IV : Pouvoirs des agents des douanes

Section 3 : Droit de communication

Paragraphe 2 : Droit de communication particulier à l'administration des douanes.

- **Article 65 quinquies**

Version en vigueur depuis le 27 décembre 2020

Modifié par LOI n°2020-1672 du 24 décembre 2020 - art. 30 (V)

Dans le but de constater les délits mentionnés aux articles 414, 414-2, 415 et 459, d'en rassembler les preuves et d'en rechercher les auteurs, les complices ainsi que ceux qui y ont participé comme intéressés au sens de l'article 399, les agents des douanes ayant au moins le grade de contrôleur et spécialement habilités par le directeur du service auquel ils sont affectés peuvent se faire communiquer les données conservées et traitées par les opérateurs de communications électroniques dans le cadre de l'article L. 34-1 du code des postes et des communications électroniques ainsi que par les prestataires mentionnés 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.

La mise en œuvre du droit de communication prévu au premier alinéa du présent article est préalablement autorisée par le procureur de la République près le tribunal judiciaire du lieu de la direction des douanes dont dépend le service chargé de la procédure.

L'autorisation du procureur de la République, qui peut être donnée par tout moyen, est mentionnée ou versée au dossier de la procédure.

La communication des données mentionnées au premier alinéa fait l'objet d'un procès-verbal de constat, qui est versé au dossier de la procédure. Une copie de ce procès-verbal est transmise au procureur de la République qui a autorisé la mise en œuvre du droit de communication ainsi qu'aux opérateurs et prestataires mentionnés au même premier alinéa, au plus tard dans les cinq jours suivant son établissement.

Les données communiquées sont détruites à l'extinction de l'action pour l'application des sanctions fiscales.

Un décret en Conseil d'Etat fixe les modalités d'application du présent article.

Nota : Conformément à l'article 36 de l'ordonnance n° 2019-964 du 18 septembre 2019, ces dispositions entrent en vigueur au 1er janvier 2020.

4. Code monétaire et financier

Livre VI : Les institutions en matière bancaire et financière

Titre II : L'Autorité des marchés financiers

Chapitre unique : L'Autorité des marchés financiers

Section 4 : Pouvoirs

Sous-section 3 : Contrôles et enquêtes

- **Article L. 621-10-2**

Version en vigueur depuis le 25 octobre 2018

Création LOI n°2018-898 du 23 octobre 2018 - art. 13

Pour la recherche des abus de marché définis par le règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/ CE du Parlement européen et du Conseil et les directives 2003/124/ CE, 2003/125/ CE et 2004/72/ CE de la Commission, les enquêteurs peuvent se faire communiquer les données conservées et traitées par les opérateurs de télécommunication, dans les conditions et sous les limites prévues à l'article L. 34-1 du code des postes et des communications électroniques, et par les prestataires mentionnés 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.

La communication des données mentionnées au premier alinéa du présent article fait l'objet d'une autorisation préalable par un contrôleur des demandes de données de connexion.

Le contrôleur des demandes de données de connexion est, en alternance, un membre du Conseil d'Etat, en activité ou honoraire, élu par l'assemblée générale du Conseil d'Etat, puis un magistrat de la Cour de cassation, en activité ou honoraire, élu par l'assemblée générale de ladite Cour. Son suppléant, issu de l'autre juridiction, est désigné selon les mêmes modalités. Le contrôleur des demandes de données de connexion et son suppléant sont élus pour une durée de quatre ans non renouvelable.

Il ne peut être mis fin aux fonctions du contrôleur des demandes de données de connexion que sur sa demande ou en cas d'empêchement constaté, selon le cas, par le vice-président du Conseil d'Etat ou par le premier président de la Cour de cassation ou le procureur général près ladite Cour, sur saisine du ministre chargé de l'économie.

Le contrôleur des demandes de données de connexion ne peut recevoir ou solliciter aucune instruction de l'Autorité des marchés financiers ni d'aucune autre autorité dans l'exercice de sa mission. Il est tenu au secret professionnel dans les conditions prévues à l'article L. 621-4 du présent code.

Il est saisi par demande motivée du secrétaire général ou du secrétaire général adjoint de l'Autorité des marchés financiers. Cette demande comporte les éléments de nature à en justifier le bien-fondé.

L'autorisation est versée au dossier d'enquête.

Les enquêteurs utilisent les données communiquées par les opérateurs de télécommunication et les prestataires mentionnés au premier alinéa du présent article exclusivement dans le cadre de l'enquête au titre de laquelle ils ont reçu l'autorisation.

Les données de connexion relatives aux faits faisant l'objet de notifications de griefs par le collège de l'Autorité des marchés financiers sont détruites à l'expiration d'un délai de six mois à compter de la décision définitive de la commission des sanctions ou des juridictions de recours. En cas de composition administrative, le délai de six mois court à compter de l'exécution de l'accord.

Les données de connexion relatives à des faits n'ayant pas fait l'objet d'une notification de griefs par le collège de l'Autorité des marchés financiers sont détruites à l'expiration d'un délai d'un mois à compter de la décision du collège.

En cas de transmission du rapport d'enquête au procureur de la République financier ou en cas de mise en mouvement de l'action publique par le procureur de la République financier en application des III et IV de l'article L. 465-3-6, les données de connexion sont remises au procureur de la République financier et ne sont pas conservées par l'Autorité des marchés financiers.

Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat.

5. Code de procédure pénale

Livre Ier : De la conduite de la politique pénale, de l'exercice de l'action publique et de l'instruction

Titre II : Des enquêtes et des contrôles d'identité

Chapitre Ier : Des crimes et des délits flagrants

- **Article 60-1**

Version en vigueur depuis le 25 mars 2019

Modifié par LOI n°2019-222 du 23 mars 2019 - art. 47 (V)

Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord.

A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros.

A peine de nullité, ne peuvent être versés au dossier les éléments obtenus par une réquisition prise en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

- **Article 60-2**

Modifié par LOI n°2019-222 du 23 mars 2019 - art. 47 (V)

Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 16

Sur demande de l'officier de police judiciaire, ou sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au d du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 précité et au 2° de l'article 80 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire ou, sous le contrôle de ce dernier, de l'agent de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 euros.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises.

Nota : Conformément à l'article 29 de l'ordonnance n° 2018-1125 du 12 décembre 2018, ces dispositions entrent en vigueur en même temps que le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au 1er juin 2019.

Chapitre II : De l'enquête préliminaire

- **Article 77-1-1**

Version en vigueur du 27 décembre 2020 au 01 mars 2022
Modifié par Décision n°2021-952 QPC du 3 décembre 2021, v. init.
Modifié par LOI n°2020-1672 du 24 décembre 2020 - art. 26

Le procureur de la République ou, sur autorisation de celui-ci, l'officier ou l'agent de police judiciaire, peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord.

En cas d'absence de réponse de la personne aux réquisitions, les dispositions du second alinéa de l'article 60-1 sont applicables.

Le dernier alinéa de l'article 60-1 est également applicable.

Le procureur de la République peut, par la voie d'instructions générales prises en application de l'article 39-3, autoriser les officiers ou agents de police judiciaire, pour des catégories d'infractions qu'il détermine, à requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique, de leur remettre des informations intéressant l'enquête qui sont issues d'un système de vidéoprotection. Le procureur est avisé sans délai de ces réquisitions. Ces instructions générales ont une durée qui ne peut excéder six mois. Elles peuvent être renouvelées.

Nota : Par une décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel a déclaré contraires à la Constitution les mots ", y compris celles issues d'un système informatique ou d'un traitement de données nominatives, " figurant à la première phrase du premier alinéa de l'article 77-1-1 du code de procédure pénale, dans sa rédaction résultant de la loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée, et " aux réquisitions prévues par le premier alinéa de l'article 60-2 " figurant au premier alinéa de l'article 77-1-2 du même code, dans sa rédaction résultant de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. L'abrogation de ces dispositions est toutefois reportée au 31 décembre 2022. Les mesures prises avant cette date en application des dispositions déclarées contraires à la Constitution ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

- **Article 77-1-2**

Modifié par Décision n°2021-952 QPC du 3 décembre 2021, v. init.
Modifié par LOI n°2019-222 du 23 mars 2019 - art. 47 (V)

Sur autorisation du procureur de la République, l'officier ou l'agent de police judiciaire peut procéder aux réquisitions prévues par le premier alinéa de l'article 60-2.

Sur autorisation du juge des libertés et de la détention saisi à cette fin par le procureur de la République, l'officier ou l'agent de police peut procéder aux réquisitions prévues par le deuxième alinéa de l'article 60-2.

Les organismes ou personnes concernés mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni conformément aux dispositions du quatrième alinéa de l'article 60-2.

Nota : Par une décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel a déclaré contraires à la Constitution les mots ", y compris celles issues d'un système informatique ou d'un traitement de données nominatives, " figurant à la première phrase du premier alinéa de l'article 77-1-1 du code de procédure pénale, dans sa rédaction résultant de la loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée, et " aux réquisitions prévues par le premier alinéa de l'article 60-2 " figurant au premier alinéa de l'article 77-1-2 du même code, dans sa rédaction résultant de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. L'abrogation de ces dispositions est toutefois reportée au 31 décembre 2022. Les mesures prises avant cette date en application des dispositions déclarées contraires à la Constitution ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

6. Livre des procédures fiscales

- **Article L. 96 G**

Version en vigueur depuis le 01 janvier 2022

Modifié par LOI n°2021-1900 du 30 décembre 2021 - art. 145

I. – Pour les besoins de la recherche ou de la constatation des infractions mentionnées au c du 1 de l'article 1728, aux b et c de l'article 1729, au I de l'article 1729-0 A et au dernier alinéa de l'article 1758 du code général des impôts, des agents de l'administration des impôts ayant au moins le grade de contrôleur et spécialement habilités par le directeur du service auquel ils sont affectés ou son adjoint peuvent, dans les conditions prévues au II du présent article, se faire communiquer les données conservées et traitées par les opérateurs de communications électroniques dans le cadre de l'article L. 34-1 du code des postes et des communications électroniques et par les prestataires mentionnés 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 dans les conditions prévues au même article 6.

II.-La mise en œuvre du droit de communication mentionné au I fait l'objet d'une autorisation préalable par un contrôleur des demandes de données de connexion.

Le contrôleur des demandes de données de connexion est, en alternance, un membre du Conseil d'Etat, en activité ou honoraire, élu par l'assemblée générale du Conseil d'Etat, et un magistrat de la Cour de cassation, en activité ou honoraire, élu par l'assemblée générale de la Cour de cassation. Son suppléant, issu de l'autre juridiction, est désigné selon les mêmes modalités. Le contrôleur des demandes de données de connexion et son suppléant sont élus pour une durée de quatre ans non renouvelable.

Il ne peut être mis fin aux fonctions du contrôleur des demandes de données de connexion que sur sa demande ou en cas d'empêchement constaté, selon le cas, par le vice-président du Conseil d'Etat ou par le premier président de la Cour de cassation ou le procureur général près cette Cour, sur saisine du ministre chargé du budget.

Le contrôleur des demandes de données de connexion ne peut recevoir ni solliciter aucune instruction de la direction générale des finances publiques, ni d'aucune autre autorité dans l'exercice de sa mission.

Il est saisi par demande motivée du directeur, ou de son adjoint, du service mentionné au I. Cette demande comporte les éléments de nature à en justifier le bien-fondé.

L'autorisation est versée au dossier de la procédure.

Les informations communiquées à l'administration sont détruites au plus tard à l'issue d'un délai d'un an à compter de leur réception, à l'exception de celles utilisées dans le cadre de l'une des procédures prévues au présent titre qui sont détruites à l'expiration de toutes les voies de recours.

Les modalités d'application du I et du présent II sont fixées par décret en Conseil d'Etat.

III. – Les agents de l'administration des impôts peuvent se faire communiquer les données traitées et conservées relatives à l'identification du vendeur ou du prestataire, à la nature des biens ou des services vendus, à la date et au montant des ventes ou prestations effectuées par les opérateurs des services prévus au d du 2 de l'article 7 du règlement d'exécution (UE) n° 282/2011 du Conseil du 15 mars 2011 portant mesures d'exécution de la directive 2006/112/ CE relative au système commun de taxe sur la valeur ajoutée

7. Code de la sécurité intérieure

LIVRE VIII : DU RENSEIGNEMENT

TITRE V : DES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT SOUMISES A AUTORISATION

Chapitre Ier : Des accès administratifs aux données de connexion

- **Article L. 851-1**

Création LOI n°2015-912 du 24 juillet 2015 - art. 5

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.

Par dérogation à l'article L. 821-2, les demandes écrites et motivées portant sur les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée sont directement transmises à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement mentionnés aux articles L. 811-2 et L. 811-4. La commission rend son avis dans les conditions prévues à l'article L. 821-3.

Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux informations ou documents collectés.

Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des techniques de renseignement.

- **Article L. 851-2**

Version en vigueur depuis le 31 juillet 2021

Modifié par LOI n°2021-998 du 30 juillet 2021 - art. 16

Modifié par LOI n°2021-998 du 30 juillet 2021 - art. 18

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 susceptible d'être en lien avec une menace, ainsi que des adresses complètes de ressources sur internet utilisées par cette personne. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.

I bis.-Le nombre maximal des autorisations délivrées en application du présent article en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.

II.-(abrogé)

8. Code du travail

- **Article L. 8113-5-2**

Version en vigueur depuis le 07 septembre 2018

Création LOI n°2018-771 du 5 septembre 2018 - art. 103

Pour la recherche et la constatation des infractions constitutives de travail illégal mentionnées à l'article L. 8211-1, les agents de contrôle définis par voie règlementaire disposent d'un droit de communication leur permettant d'obtenir, sans que s'y oppose le secret professionnel, communication de tout document, renseignement ou élément d'information utile à l'accomplissement de leur mission.

Sans préjudice des autres dispositions législatives applicables en matière d'échanges d'informations, le droit de communication défini au présent article est exercé dans les conditions prévues et auprès des personnes mentionnées à la section I du chapitre II du titre II de la première partie du livre des procédures fiscales, à l'exception des personnes mentionnées aux articles L. 82 C, L. 83 A à L. 83 E, L. 84 à L. 84 E, L. 91, L. 95 et L. 96 B à L. 96 F du même livre.

Pour les données conservées et traitées par les opérateurs de communications électroniques dans le cadre de l'article L. 34-1 du code des postes et des communications électroniques et par les prestataires mentionnés 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, le droit de communication institué par le présent article ne s'applique qu'aux seules données permettant l'identification des personnes proposant un travail, une prestation ou une activité pouvant relever des infractions constitutives de travail illégal mentionnées à l'article L. 8211-1 du présent code.

Le droit de communication prévu au premier alinéa du présent article s'exerce quel que soit le support utilisé pour la conservation des documents et peut s'accompagner de la prise d'extraits et de copies. Les documents et informations sont communiqués à titre gratuit dans les trente jours qui suivent la réception de la demande écrite.

Il peut porter sur des informations relatives à des personnes non identifiées, dans des conditions fixées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

9. 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)

- **Article 15**

Application de certaines dispositions de la directive 95/46/CE

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

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques.

D. Application des dispositions contestées et d'autres dispositions

1. Jurisprudence

a. Jurisprudence communautaire

- **CJUE, (grande chambre) du 8 avril 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, aff. C 293/12 et C-594/12.**

Sur la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte

38 Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés 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.

39 En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte, il convient de constater que, même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1er, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

40 Cette conservation des données n'est pas non plus de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, sans préjudice des dispositions adoptées en application des directives 95/46 et 2002/58, certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, principes selon lesquels les États membres veillent à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

41 Quant à la question de savoir si ladite ingérence répond à un objectif d'intérêt général, il convient de relever que, si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

42 Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU:C:2008:461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU:C:2012:711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU:C:2010:708, points 46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté.

43 À cet égard, il ressort du considérant 7 de la directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil «Justice et affaires intérieures» du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.

44 Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24, répond effectivement à un objectif d'intérêt général.

45 Dans ces conditions, il y a lieu de vérifier la proportionnalité de l'ingérence constatée.

46 À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (voir, en ce sens, arrêts Afton Chemical, C-343/09, EU:C:2010:419, point 45; Volker und Markus

Schecke et Eifert, EU:C:2010:662, point 74; Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, point 71; Sky Österreich, C-283/11, EU:C:2013:28, point 50, ainsi que Schaible, C-101/12, EU:C:2013:661, point 29).

47 En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt Cour EDH, S et Marper c. Royaume-Uni [GC], nos 30562/04 et 30566/04, § 102, CEDH 2008-V).

48 En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données a' caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

49 En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

50 Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

51 En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

52 S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

53 À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci.

54 Ainsi, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, no 58243/00, § 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

55 La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, S et Marper c. Royaume-Uni, précité, § 103, ainsi que M. K. c. France, no 19522/09, § 35, du 18 avril 2013).

56 Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous

les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

57 À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

58 En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59 D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

60 En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

61 En outre, quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

62 En particulier, la directive 2006/24 ne prévoit 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. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.

63 En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

64Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

65 Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

66 De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées

contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles.

67 L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

68 En second lieu, il convient d'ajouter que ladite directive n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir, en ce sens, arrêt Commission/Autriche, C-614/10, EU:C:2012:631, point 37).

69 Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte.

- **<u>CJUE, (grande chambre) du 21 décembre 2016, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a, aff. C-203/15 et C-698/15</u>**

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, au regard des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte

82 Il convient de relever que, conformément à l'article 1er, paragraphe 2, de la directive 2002/58, les dispositions de celle-ci « précisent et complètent » la directive 95/46. Ainsi que l'énonce son considérant 2, la directive 2002/58 vise à garantir, en particulier, le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ».

83 À cette fin, la directive 2002/58 contient des dispositions spécifiques visant, ainsi qu'il ressort notamment de ses considérants 6 et 7, à protéger les utilisateurs des services de communications électroniques contre les dangers pour les données à caractère personnel et la vie privée résultant des nouvelles technologies et de la capacité accrue de stockage et de traitement automatisés de données.

84 En particulier, l'article 5, paragraphe 1, de cette directive prévoit que les États membres doivent garantir, par leur 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.

85 Le principe de confidentialité des communications instauré par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, paragraphe 1, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, paragraphe 1, de cette directive et le stockage technique nécessaire à l'acheminement d'une communication (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae,C-275/06, EU:C:2008:54, point 47).

86 Ainsi, et comme le confirment les considérants 22 et 26 de la directive 2002/58, le traitement et le stockage des données relatives au trafic ne sont autorisés, en vertu de l'article 6 de cette directive, que dans la mesure et pour la durée nécessaires à la facturation des services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae,C-275/06, EU:C:2008:54, points

47 et 48). S'agissant, en particulier, de la facturation des services, un tel traitement n'est autorisé que 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. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. S'agissant des données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés.

87 La portée des dispositions des articles 5 et 6 et de l'article 9, paragraphe 1, de la directive 2002/58, qui visent à garantir la confidentialité des communications et des données y afférentes ainsi qu'à minimiser les risques d'abus, doit en outre être appréciée à la lumière du considérant 30 de cette directive, aux termes duquel « [l]es systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires ».

88 Certes, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae,C-275/06, EU:C:2008:54, point 50).

89 Néanmoins, en ce que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres de limiter la portée de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, il est, conformément à la jurisprudence constante de la Cour, d'interprétation stricte (voir, par analogie, arrêt du 22 novembre 2012, Probst,C-119/12, EU:C:2012:748, point 23). Une telle disposition ne saurait donc justifier que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de cette directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée.

90 Il convient, à cet égard, de relever que l'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les mesures législatives qu'il vise et qui dérogent au principe de confidentialité des communications et des données relatives au trafic y afférentes doivent avoir pour objectif de « sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou [d']assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques », ou doivent poursuivre un des autres objectifs visés à l'article 13, paragraphe 1, de la directive 95/46, auquel renvoie l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae,C-275/06, EU:C:2008:54, point 53). Une telle énumération d'objectifs revêt un caractère exhaustif ainsi qu'il ressort de l'article 15, paragraphe 1, deuxième phrase, de cette dernière directive, aux termes duquel les mesures législatives doivent être justifiées par « un des motifs énoncés » à l'article 15, paragraphe 1, première phrase, de ladite directive. Partant, les États membres ne sauraient adopter de telles mesures à d'autres fins que celles énumérées à cette dernière disposition.

91 En outre, l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 dispose que « [t]outes les mesures visées [à l'article 15, paragraphe 1, de cette directive] sont prises dans le respect des principes généraux du droit [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, [UE] », parmi lesquels figurent les principes généraux et les droits fondamentaux qui sont désormais garantis par la Charte. L'article 15, paragraphe 1, de la directive 2002/58 doit ainsi être interprété à la lumière des droits fondamentaux garantis par la Charte (voir, par analogie, en ce qui concerne la directive 95/46, arrêts du 20 mai 2003, Österreichischer Rundfunk e.a.,C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 68 ; du 13 mai 2014, Google Spain et Google, C-131/12, EU:C:2014:317, point 68, ainsi que du 6 octobre 2015, Schrems,C-362/14, EU:C:2015:650, point 38).

92 À cet égard, il importe de souligner que l'obligation faite aux fournisseurs de services de communications électroniques, par une réglementation nationale telle que celle en cause au principal, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, qui sont explicitement mentionnés dans les questions préjudicielles, mais également de la liberté d'expression garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 25 et 70).

93 Ainsi, l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour (voir, en ce sens, arrêt du 6 octobre 2015, Schrems,C-362/14, EU:C:2015:650, point 39 et jurisprudence citée), doit être prise en compte lors de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58. Il en va de même du droit à la liberté d'expression eu égard à l'importance particulière que revêt cette liberté dans toute société démocratique. Ce droit fondamental, garanti à l'article 11 de la Charte, constitue l'un des fondements essentiels d'une société démocratique et pluraliste, faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 12 juin 2003, Schmidberger,C-112/00, EU:C:2003:333, point 79, et du 6 septembre 2011, Patriciello,C-163/10, EU:C:2011:543, point 31).

94 À cet égard, il convient de rappeler que, conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés reconnus par celle-ci doit être prévue par la loi et respecter leur contenu essentiel. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à l'exercice de ces droits et de ces libertés 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 des libertés d'autrui (arrêt du 15 février 2016, N.,C-601/15 PPU, EU:C:2016:84, point 50).

95 À ce dernier égard, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'elle est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Quant au considérant 11 de cette directive, il précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi. En ce qui concerne, en particulier, la conservation de données, l'article 15, paragraphe 1, deuxième phrase, de ladite directive exige que celle-ci n'ait lieu que « pendant une durée limitée » et « lorsque cela est justifié » par un des objectifs visés à l'article 15, paragraphe 1, première phrase, de cette même directive.

96 Le respect du principe de proportionnalité découle également de la jurisprudence constante de la Cour selon laquelle la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 77 ; Digital Rights, point 52, ainsi que du 6 octobre 2015, Schrems,C-362/14, EU:C:2015:650, point 92).

97 S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause dans l'affaire C-203/15, satisfait à ces conditions, il convient de relever que celle-ci prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Ainsi qu'il ressort de la décision de renvoi, les catégories de données visées par cette réglementation correspondent, en substance, à celles dont la conservation était prévue par la directive 2006/24.

98 Les données que doivent ainsi conserver les fournisseurs de services de communications électroniques permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile. Au nombre de ces données figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 26).

99 Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 27). En particulier, ces données fournissent les moyens d'établir, ainsi que l'a relevé M. l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions, le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

100 L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37).

101 Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 39), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique

et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28).

102 Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 60).

103 En outre, si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 51).

104 À cet égard, il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception.

105 D'autre part, une réglementation nationale telle que celle en cause au principal, qui couvre de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 57 et 58).

106 Une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 59).

107 Une réglementation nationale telle que celle en cause au principal excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

108 En revanche, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

109 Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 54 et jurisprudence citée).

110 En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif

poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

111 S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les 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 la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

112 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la première question dans l'affaire C-203/15 que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

(….)

Par ces motifs, la Cour (grande chambre) dit pour droit :

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 une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

2)

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 s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

- **<u>CJUE, (grande chambre) du 2 octobre 2018, *Ministerio Fiscal*, aff. C-207/16</u>**

Sur le fond

48 Par ses deux questions, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui présente une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave et, dans l'affirmative, à l'aune de quels critères la gravité de l'infraction en cause doit être appréciée.

49 À cet égard, il ressort de la décision de renvoi que, comme l'a relevé en substance M. l'avocat général au point 38 de ses conclusions, la demande de décision préjudicielle ne vise pas à déterminer si les données à caractère personnel en cause au principal ont été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la directive 2002/58, lu à la

lumière des articles 7 et 8 de la Charte. Cette demande porte, ainsi qu'il ressort du point 46 du présent arrêt, uniquement sur la question de savoir si et dans quelle mesure l'objectif poursuivi par la réglementation en cause au principal est susceptible de justifier l'accès d'autorités publiques, telles que la police judiciaire, à de telles données, sans que les autres conditions d'accès résultant de cet article 15, paragraphe 1, fassent l'objet de cette demande.

50 En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238), et Tele2 Sverige et Watson e.a.

51 Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que, comme l'a relevé M. l'avocat général aux points 76 et 77 de ses conclusions, l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de « grave » et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée].

52 En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 90 et 115).

53 Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général.

54 À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 99).

55 La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 115).

56 En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ».

57 En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général.

58 Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en cause au principal comporterait doit être considérée comme étant « grave ».

59 À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu'il a été relevé au point 40 du présent arrêt, cette demande vise l'accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60 Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61 Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées.

62 Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves ».

63 Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

- **CJUE, (grande chambre) du 6 octobre 2020, *La Quadrature du Net e.a. contre Premier ministre e.a.*, aff. C 511 /18**

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58

105 Il convient de rappeler, à titre liminaire, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (voir, en ce sens, arrêt du 17 avril 2018, Egenberger, C-414/16, EU:C:2018:257, point 44).

106 La directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé

des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ».

107 À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données.

108 S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 86 et jurisprudence citée).

109 Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110 Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. 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 l'un de ces motifs.

111 Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104).

112 Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 52 et jurisprudence citée).

113 En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non

seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

114 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 39, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

115 Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée ; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, Breyer c. Allemagne, CE:ECHR:2020:0130JUD005000112, § 81].

116 Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, § 69, ainsi que 13 février 2020, Trjakovski et Chipovski c. Macédonie du Nord, CE:ECHR:2020:0213JUD005320513, § 51), l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

117 Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 99).

118 Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 28, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations

du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119 D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120 Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

121 En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

122 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123 À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 47 ; du 28 juillet 2016, JZ, C-294/16 PPU, EU:C:2016:610, point 48, ainsi que du 19 septembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, point 42 et jurisprudence citée).

124 En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18 PPU, EU:C:2019:108, point 57, ainsi que du 21 mai 2019, Commission/Hongrie (Usufruits sur terres agricoles), C-235/17, EU:C:2019:432, point 72 et jurisprudence citée].

125 S'agissant de l'article 5 de la CEDH, qui consacre le « droit à la liberté » et le « droit à la sûreté », celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, Ladent c. Pologne, CE:ECHR:2008:0318JUD001103603, §§ 45 et 46 ; 29 mars 2010, Medvedyev et autres c. France, CE:ECHR:2010:0329JUD000339403, §§ 76 et 77, ainsi que 13 décembre 2012, El-Masri v. « The former Yugoslav Republic of Macedonia », CE:ECHR:2012:1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126 En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative), C-78/18, EU:C:2020:476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également

susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127 Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128 En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, §§ 115 et 116 ; 4 mars 2004, M.C. c. Bulgarie, CE:ECHR:2003:1204JUD003927298, § 151 ; 24 juin 2004, Von Hannover c. Allemagne, CE:ECHR:2004:0624JUD005932000, §§ 57 et 58, ainsi que 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 et 49).

129 En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi.

130 À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

131 Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée).

132 Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du

8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 117 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

133 Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63].

– Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale

134 Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la directive 2002/58.

135 À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État 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'État en tant que tel, telles que notamment des activités de terrorisme.

136 Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

137 Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138 L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139 Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la

sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse 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.

(…)

168 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre 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 que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, 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, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, 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, au moyen 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.

- **<u>CJUE, (grande chambre) du 2 mars 2021, *Prokuratuur,* aff. C-746/18</u>**

Sur les première et deuxième questions

27 Par ses première et deuxième questions préjudicielles, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la

lutte contre la criminalité grave, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité, de la quantité ainsi que de la nature des données disponibles pour une telle période.

28 À cet égard, il ressort de la demande de décision préjudicielle que, comme l'a confirmé le gouvernement estonien lors de l'audience, les données auxquelles l'autorité nationale chargée de l'enquête a eu accès dans l'affaire au principal sont celles retenues en vertu de l'article 1111, paragraphes 2 et 4, de la loi relative aux communications électroniques imposant aux fournisseurs de services de communications électroniques une obligation de conserver de manière généralisée et indifférenciée les données relatives au trafic et les données de localisation en ce qui concerne la téléphonie fixe et mobile, pendant un an. Ces données permettent, notamment, de retrouver et d'identifier la source et la destination d'une communication à partir du téléphone fixe ou mobile d'une personne, de déterminer la date, l'heure, la durée et la nature de cette communication, d'identifier le matériel de communication utilisé ainsi que de localiser le téléphone mobile sans qu'une communication soit nécessairement acheminée. En outre, elles offrent la possibilité de déterminer la fréquence des communications de l'utilisateur avec certaines personnes pendant une période donnée. Par ailleurs, comme l'a confirmé le gouvernement estonien lors de l'audience, l'accès auxdites données peut, en matière de lutte contre la criminalité, être sollicité pour tout type d'infraction pénale.

29 S'agissant des conditions dans lesquelles l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques peut, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, être accordé à des autorités publiques, en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, la Cour a jugé qu'un tel accès ne peut être octroyé que pour autant que ces données aient été conservées par ces fournisseurs d'une manière conforme audit article 15, paragraphe 1 (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 167).

30 À cet égard, la Cour a également jugé que ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à des mesures législatives prévoyant, à de telles fins, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168).

31 Quant aux objectifs susceptibles de justifier un accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques en application d'une mesure conforme à ces dispositions, il ressort, d'une part, de la jurisprudence de la Cour qu'un tel accès ne peut être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs de services (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 166).

32 D'autre part, la Cour a jugé que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 131 ainsi que jurisprudence citée).

33 En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause au principal, conformément au principe de proportionnalité, seule la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif, poursuivi par la réglementation en cause au principal, de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 140 ainsi que 146).

34 À cet égard, il a notamment été jugé que les mesures législatives visant le traitement des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques en tant que telles, notamment leur conservation et l'accès à celles-ci, à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58. En effet, 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 pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées des utilisateurs des moyens de communications électroniques, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une mesure visant ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 157 et 158 ainsi que jurisprudence citée).

35 Dans ces conditions, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées (voir, en ce sens, arrêt du 2 octobre 2018,Ministerio Fiscal, C-207/16, EU:C:2018:788, point 54), sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès.

36 Il y a lieu de relever que l'accès à un ensemble de données relatives au trafic ou de données de localisation, telles que celles conservées en vertu de l'article 1111 de la loi relative aux communications électroniques, est effectivement susceptible de permettre de tirer des conclusions précises, voire très précises, concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 117).

37 Certes, ainsi que le suggère la juridiction de renvoi, plus la durée de la période pour laquelle l'accès est sollicité est longue, plus importante est, en principe, la quantité de données susceptibles d'être conservées par les fournisseurs de services de communications électroniques, concernant les communications électroniques passées, les lieux de séjour fréquentés ainsi que les déplacements effectués par l'utilisateur d'un moyen de communication électronique, permettant ainsi de tirer, à partir des données consultées, un plus grand nombre de conclusions sur la vie privée de cet utilisateur. Un constat analogue peut être tiré en ce qui concerne les catégories de données sollicitées.

38 C'est donc pour satisfaire à l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 130 ainsi que jurisprudence citée), qu'il appartient aux autorités nationales compétentes d'assurer, dans chaque cas d'espèce, que tant la ou les catégories de données visées que la durée pour laquelle l'accès à celles-ci est sollicité soient, en fonction des circonstances de l'espèce, limitées à ce qui est strictement nécessaire aux fins de l'enquête en cause.

39 Toutefois, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès, par une autorité publique, à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise, présente en tout état de cause un caractère grave indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période, lorsque, comme dans l'affaire au principal, cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées.

40 À cet égard, même l'accès à une quantité limitée de données relatives au trafic ou de données de localisation ou l'accès à des données pour une courte période peut être susceptible de fournir des informations précises sur la vie privée d'un utilisateur d'un moyen de communication électronique. En outre, la quantité des données disponibles et les informations concrètes sur la vie privée de la personne concernée en découlant sont des circonstances qui ne peuvent être appréciées qu'après la consultation desdites données. Or, l'autorisation d'accès accordée par la juridiction ou l'autorité indépendante compétente intervient nécessairement avant que les données et les informations en découlant puissent être consultées. Ainsi, l'appréciation de la gravité de l'ingérence que constitue l'accès s'effectue nécessairement en fonction du risque généralement afférent à la catégorie de données sollicitées pour la vie privée des personnes concernées, sans qu'il importe, par ailleurs, de savoir si les informations relatives à la vie privée en découlant présentent ou non, concrètement, un caractère sensible.

41 Enfin, compte tenu du fait que la juridiction de renvoi est saisie d'une demande concluant à l'irrecevabilité des procès-verbaux établis à partir des données relatives au trafic et des données de localisation, au motif que les dispositions de l'article 1111 de la loi relative aux communications électroniques seraient contraires à l'article 15, paragraphe 1, de la directive 2002/58 tant en ce qui concerne la conservation des données que l'accès à celles-ci, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, d'informations et d'éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée de ces données, contraire au droit de l'Union (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 222), ou encore par un accès des autorités nationales auxdites données, contraire à ce droit.

42 En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 223 ainsi que jurisprudence citée).

43 Pour ce qui est plus particulièrement du principe d'effectivité, il convient de rappeler que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 225).

44 La nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable. Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation. Partant, le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 226 et 227).

45 Eu égard aux considérations qui précèdent, il convient de répondre aux première et deuxième questions que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.

b. Jurisprudence administrative

- **Conseil d'Etat, 10ème - 9ème chambres réunies, 26 juillet 2018, n° 394922**

Sur les moyens de légalité externe :

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

Sur les moyens de légalité interne :

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

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

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

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

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

5. Par sa décision n° 2016-590 QPC du 21 octobre 2016, le Conseil constitutionnel a déclaré l'article L. 811-5 du code de la sécurité intérieure contraire au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789. Le dispositif de cette décision énonce que la déclaration d'inconstitutionnalité prend effet dans les conditions prévues aux paragraphes 11 et 12. Aux termes de ces paragraphes : " L'abrogation immédiate de l'article L. 811-5 du code de la sécurité intérieure aurait pour effet de priver les pouvoirs publics de toute possibilité de surveillance des transmissions empruntant la voie hertzienne. Elle entraînerait des conséquences manifestement excessives. Afin de permettre au législateur de remédier à l'inconstitutionnalité constatée, il y a donc lieu de reporter au 31 décembre 2017 la date de cette abrogation. / Afin

de faire cesser l'inconstitutionnalité constatée à compter de la publication de la présente décision, il y a lieu de juger que, jusqu'à l'entrée en vigueur d'une nouvelle loi ou, au plus tard, jusqu'au 30 décembre 2017, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être interprétées comme pouvant servir de fondement à des mesures d'interception de correspondances, de recueil de données de connexion ou de captation de données informatiques soumises à l'autorisation prévue au titre II ou au chapitre IV du titre V du livre VIII du code de la sécurité intérieure. Pendant le même délai, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être mises en oeuvre sans que la Commission nationale de contrôle des techniques de renseignement soit régulièrement informée sur le champ et la nature des mesures prises en application de cet article ". Alors même que, selon les motifs de la décision du Conseil constitutionnel, la déclaration d'inconstitutionnalité doit, en principe, bénéficier à l'auteur de la question prioritaire de constitutionnalité, l'absence de prescriptions relatives à la remise en cause des effets produits par l'article L. 811-5 du code de la sécurité intérieure avant son abrogation doit, en l'espèce, eu égard, d'une part, à la circonstance que la question prioritaire de constitutionnalité a été soulevée à l'occasion de recours pour excès de pouvoir dirigés contre des actes réglementaires, d'autre part, à la circonstance que le Conseil constitutionnel a décidé de reporter dans le temps les effets abrogatifs de sa décision, être regardée comme indiquant que le Conseil constitutionnel n'a pas entendu remettre en cause les effets que la disposition déclarée contraire à la Constitution avait produits avant la date de son abrogation. Il s'ensuit que, alors même que les associations requérantes sont les auteurs de la question prioritaire de constitutionnalité, la déclaration d'inconstitutionnalité de l'article L. 811-5 du code de la sécurité intérieure est, en tout état de cause, sans incidence sur l'issue des présents litiges dirigés contre les quatre décrets mentionnés au point 1.

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

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

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

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

8. Les dispositions des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure prévoient les conditions dans lesquelles le Conseil d'Etat est compétent pour connaître des requêtes concernant la mise en oeuvre des techniques de renseignement soumises à autorisation. Il peut être saisi soit par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en oeuvre et justifiant d'avoir au préalable saisi la Commission nationale de contrôle des techniques de renseignement sur le fondement de l'article L. 833-4 du même code, soit par le président de cette commission, ou trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes. S'agissant des mesures de surveillance des communications électroniques internationales encadrées par le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, si la personne qui pense faire l'objet d'une telle mesure de surveillance ne peut directement saisir un juge pour en contester la régularité, elle peut en revanche, sur le fondement des dispositions de l'article L. 854-9 de ce code, former une réclamation à cette fin auprès de la Commission nationale de contrôle des techniques de renseignement. Or, ce même article prévoit que lorsque la commission identifie un manquement, de sa propre initiative ou à la suite d'une telle réclamation, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin et que les renseignements collectés soient, le cas échéant, détruits. Elle peut également saisir le Conseil d'Etat.

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

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

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

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

13. Eu égard, d'une part, aux attributions de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante à laquelle il appartient de vérifier, sous le contrôle du juge, que les techniques de recueil de renseignement sont mises en oeuvre, sur le territoire national, conformément aux exigences découlant du code de la sécurité intérieure, et, d'autre part, au recours effectif ouvert, dans les conditions décrites aux points précédents, devant la formation spécialisée du Conseil d'Etat, la circonstance que les dispositions législatives contestées ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet, une fois ces dernières levées, ne caractérise pas, par elle-même, une atteinte excessive portée au droit au respect de la vie privée.

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

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

15. Les dispositions de l'article L. 851-3 du code de la sécurité intérieure permettent d'imposer aux opérateurs de communications électroniques et aux prestataires techniques " la mise en oeuvre sur leurs réseaux de traitements automatisées destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ". Cette technique vise uniquement à recueillir pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces personnes, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, ces dispositions, qui n'imposent pas une obligation générale de surveillance active, ne méconnaissent pas les dispositions claires de l'article 15 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui

prévoient que " Les Etats membres ne doivent pas imposer aux prestataires, pour la fourniture des services de simple transport, de stockage et d'hébergement une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ". Il s'ensuit qu'en tout état de cause, le moyen tiré de la méconnaissance de la directive du 8 juin 2000 doit être écarté.

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

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

17. D'autre part, la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des Etats membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le " traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté ". Mais, ainsi que le rappelle son article 1er, paragraphe 3, elle " ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ". Par ailleurs, son article 15 prévoit que " Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ". Les Etats membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive.

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

18. Il résulte des dispositions précitées de la directive du 12 juillet 2002, ainsi que l'a dit pour droit la Cour de justice de l'Union européenne par son arrêt Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres (C-203/15 et C-698/15), du 21 décembre 2016, qu'elle " doit être regardée comme régissant les activités des fournisseurs [de services de communications électroniques] ". Les dispositions imposant des obligations à ces fournisseurs, telles que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation de leurs utilisateurs et abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de la directive du 12 juillet 2002, parmi lesquelles figure la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique relèvent dès lors du champ d'application de cette directive dans la mesure où, ainsi que l'a dit pour droit la Cour de justice, elles régissent leur activité. Par ailleurs, ainsi que l'a

également dit pour droit la Cour, la circonstance que de telles obligations n'interviennent qu'aux seules fins de rendre accessibles aux autorités nationales compétentes les données personnelles qu'elles concernent, implique que la réglementation nationale encadrant l'accès et l'utilisation de ces données relève également du champ d'application de la directive du 12 juillet 2002. En revanche, les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en oeuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive.

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

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

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

Quant à l'obligation de conservation généralisée et indifférenciée :

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

23. D'une part, il est constant qu'une telle conservation préventive et indifférenciée permet aux services de renseignement d'accéder aux données relatives aux communications qu'un individu a effectuées avant que soient identifiées les raisons de penser qu'il présente une menace pour la sécurité publique, la défense ou la sûreté de l'Etat. Dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir seulement du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'Etat.

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

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

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

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

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

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

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

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

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

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

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

- **<u>Conseil d'Etat, Assemblée, 21 avril 2021, n°393099</u>**

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 nos 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 nos 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 Ier 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 nos 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 1er 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 1er 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 oeuvre 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 oeuvre 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 1er 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 oeuvre. 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 1er 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 nos 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre ". 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 oeuvre à son égard et justifiant de la mise en oeuvre 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 oeuvre 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 oeuvre 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 oeuvre. 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre, 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 oeuvre 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 oeuvre 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 oeuvre, 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 oeuvre 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 1er, 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre, 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 oeuvre 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 oeuvre 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.

c. Jurisprudence judiciaire

- **Cour de cassation, 1er avril 2020, n° 19-80908**

Sur le quatrième moyen

Enoncé du moyen

16. Le moyen est pris de la violation des articles 6, §1, et 8 de la Convention européenne des droits de l'homme, des articles 7,8 et 11 et 52 de la Charte des droits fondamentaux de l'Union européenne, de l'article 15§1 de la directive 2002/58/CE du 12 juillet 2002, des articles L. 621-10 du code monétaire et financier, des articles L. 14-1 et R. 10-13 I du code des postes et communications électroniques, de l'article 112-4 du code pénal, des articles préliminaire, 591 et 593 du même code, défaut de motifs, manque de base légale.

17. Il critique l'arrêt attaqué en ce qu'il a dit la requête mal-fondée et n'y avoir lieu à annulation d'une pièce ou d'un acte de procédure, alors :

« 1°/ que, premièrement, dès lors que l'inconventionnalité d'une disposition légale applicable au litige a été décidée par la Cour de justice de l'Union européenne, le juge national doit se prononcer conformément à la décision d'inconventionnalité ; qu'en considérant que "les dispositions de l'article L. 621-10 n'apparaissent pas contraires à l'article 15, §1, de la directive 2002/58/CE du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques" quand elle devait faire application de l'inconventionnalité de l'article L. 621-10 du code monétaire et financier, la cour d'appel a violé les textes susvisés ;

2°/ que, deuxièmement, et en tout cas, tout arrêt ou jugement doit comporter les motifs propres à justifier sa décision, que l'insuffisance de motifs équivaut à un défaut de motifs ; qu'en se fondant, pour rejeter la requête en nullité de M. T..., sur un arrêt de la CJUE du 2 octobre 2018, sans dire en quoi la jurisprudence citée et retenue par celle-ci excluait l'application au cas d'espèce de la décision d'inconventionnalité de l'article L. 621-10 du code monétaire et financier, les juges du fond ont méconnu le sens et la portée des textes susvisés. »

Réponse de la Cour

18. Pour écarter l'exception d'inconventionnalité des articles L. 621-10 du code monétaire et financier et L. 34-1 du code des postes et communications électroniques au regard des impératifs de la directive 2002/ 58/CE du 12 juillet 2002, lue à la lumière de la jurisprudence de la CJUE, les juges, après avoir rappelé les circonstances dans lesquelles ont été recueillies les données personnelles concernant notamment M. T..., relèvent que l'article L. 621-10 du code monétaire et financier, qui réserve à des agents d'une autorité administrative, habilités et soumis au respect du secret professionnel, le pouvoir d'obtenir communication des données de connexion, n'apparaissent pas contraire à l'article 15§1 de la directive précitée.

19. Ils retiennent qu'il en va de même des dispositions de l'article L.34-1 du code des postes et communications électroniques, du fait des limitations apportées par l'article R. 10-3 I, tant en ce qui concerne les données devant être conservées par les opérateurs, que la durée de leur conservation.

20. Ils soulignent que l'article 23§1 h) du règlement (UE) n°596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché permet aux autorités compétentes de se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic, détenus par un opérateur de télécommunications, lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation de l'article 14 point a) ou b), concernant l'interdiction d'effectuer ou de tenter d'effectuer des opérations d'initiés ou de recommander à une autre personne ou d'inciter une autre personne à effectuer des opérations d'initiés, ou de l'article 15, relatif à l'interdiction des manipulations de marché.

21. Les juges en déduisent qu'aucune nullité ne saurait résulter de l'application de dispositions conformes à un règlement européen, acte juridique européen, de portée générale, obligatoire dans toutes ses dispositions et directement applicable dans l'ordre juridique des Etats membres à tous les sujets de droit.

22. Pour conclure à la cassation de l'arrêt attaqué, le demandeur soutient, en substance, que c'est en violation de la directive 2002/58/CE précitée, telle qu'interprétée par la CJUE que les données ont été recueillies sur le fondement des textes précités qui organisent une conservation généralisée et indifférenciée des données et que les dispositions de l'article L. 621-10 du code monétaire et financier dans sa rédaction issue de la loi du 26 juillet 2013, ne fixent aucune limite au droit, pour des enquêteurs de l'AMF, de se faire communiquer les données conservées.

23. L'avocat général, sur ce point, conclut qu'il est nécessaire de poser à la CJUE deux questions, la première relative à la conventionnalité des conditions de conservation des données personnelles de connexion par des opérateurs privés, la seconde, sur les conditions de leur accès par l'AMF organisé par l'article L. 621-10 précité, dans sa version alors applicable, compte tenu des dispositions du règlement (UE) n° 596/2014 du 16 avril 2014 sur les abus de marché et des obligations qui en découlent pour les Etats membres, règlement qui a abrogé la directive 2003/6/CE du Parlement et du Conseil du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché.

24. En réplique, selon le demandeur, il n'y a pas lieu de saisir la CJUE d'une question préjudicielle, dès lors que cette juridiction s'est déjà prononcée clairement sur le sens de la directive 2002/58/CE du 12 juillet 2002.

25. L'examen du moyen rend nécessaire de distinguer les modalités d'accès aux données de connexion, de celles relatives à leur conservation.

Sur l'accès aux données de connexion

26. Dans sa décision Tele 2 Sverige du 21 décembre 2016 (aff. jointes C-203/15 et C- 698/15), la Cour de justice de l'Union européenne a dit pour droit que l'article 15§1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52§1 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'"il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation ... sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union" (point 125).

27. De son côte, le Conseil constitutionnel, par décision du 21 juillet 2017, a déclaré inconstitutionnel le premier alinéa de l'article L. 621-10 du code monétaire et financier au motif que la procédure d'accès par l'AMF, telle qu'elle existait à l'époque des faits, n'était pas conforme au droit au respect de la vie privée, protégée par l'article 2 de la Déclaration des droits de l'homme et du citoyen. Cependant, considérant que l'abrogation immédiate des dispositions contestées aurait des conséquences manifestement excessives, le Conseil constitutionnel a reporté cette abrogation au 31 décembre 2008. Tirant les conséquences de cette déclaration d'inconstitutionnalité, le législateur, par la loi n° 2018-898 du 23 octobre 2018 a introduit un nouvel article L. 621-10-2 instaurant la délivrance d'une autorisation préalable par une autre autorité administrative indépendante appelée "contrôleur des demandes d'accès", de tout accès aux données de connexion par les enquêteurs de l'AMF ;

28. Compte tenu du report dans le temps des effets de la décision du Conseil constitutionnel, il y a lieu de considérer qu'aucune nullité ne peut être tirée de l'inconstitutionnalité des dispositions législatives applicables à l'époque des faits. En revanche, bien que, selon l'article L. 621-1 du code monétaire et financier, tant dans sa rédaction applicable à la date des actes litigieux que dans sa rédaction actuelle, l'AMF soit "une autorité publique indépendante", la faculté offerte à ses enquêteurs d'obtenir des données de connexion sans contrôle préalable par une juridiction ou une autre autorité administrative indépendante n'était pas conforme aux exigences posées par les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, tels qu'interprétés par la CJUE.

29. La seule question qui se pose porte sur la possibilité de reporter dans le temps les conséquences de l'inconventionnalité de l'article L. 621-10 du code monétaire et financier.

Sur la conservation des données de connexion

30. Dans sa décision Tele 2 Sverige du 21 décembre 2016 (aff. jointes C-203/15 et C- 698/15) la Cour de justice de l'Union européenne a dit pour droit que l'article 15§1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52§1 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'"il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électroniques" (point 112).

31. En l'espèce, l'accès aux données conservées a été mis en oeuvre par l'AMF, qui soupçonnait des opérations d'initiés et des abus de marché susceptibles de plusieurs qualifications pénales graves, et avait besoin, pour l'efficacité de son enquête, de croiser différentes données conservées sur un certain laps de temps, permettant de mettre au jour des informations privilégiées entre plusieurs interlocuteurs, qui ont révélé l'existence de pratiques illicites en la matière.

32. Ces enquêtes menées par l'AMF répondent aux obligations mises à la charge des Etats par la directive 2003/6/CE du Parlement et du Conseil du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché (abus de marché) leur imposant de désigner une autorité administrative unique, dont les pouvoirs, définis

au point d) de l'article 12, §2, comprennent celui d'exiger "des enregistrements téléphoniques et des données échangées existants".

33. Le règlement (UE) n° 596/2014 du 16 avril 2014 sur les abus de marché, qui s'est substitué à la directive précitée à compter du 3 juillet 2016, consacre, ainsi que l'énonce son objet défini à l'article 1er, l'existence "d'un cadre réglementaire commun sur les opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché ... ainsi que des mesures visant à empêcher les abus de marché afin de garantir l'intégrité des marchés financiers de l'Union et d'accroître la protection des investisseurs et leur confiance dans ces marchés".

34. Il prévoit, en son article 23, paragraphe 2, points g) et h), que l'autorité compétente peut se faire remettre les enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic, détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières.

35. Elle peut aussi se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic, détenus par un opérateur de télécommunications lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation de l'article 14, point a) ou b), sur les opérations d'initiés et la divulgation illicite d'informations privilégiées, ou de l'article 15, sur les manipulations de marché.

36. Ce texte souligne également (considérant 65) que ces données de connexion constituent une preuve essentielle, et parfois la seule, permettant de détecter et de démontrer l'existence d'une opération d'initié ou d'une manipulation de marché, dès lors qu'elles permettent d'établir l'identité de la personne à l'origine de la diffusion d'une information fausse ou trompeuse, ou prouver que des personnes ont été en contact à un moment donné et démontrer l'existence d'une relation entre deux ou plusieurs personnes.

37. Relevant que l'exercice de tels pouvoirs peut entrer en conflit avec le droit au respect de la vie privée et familiale, du domicile et des communications, il prescrit aux Etats de prévoir des garanties appropriées et efficaces contre tout abus en limitant lesdits pouvoirs aux seuls cas où ils sont nécessaires à la conduite correcte d'une enquête sur des cas graves pour lesquels les Etats ne disposent pas de moyens équivalents leur permettant de parvenir efficacement au même résultat, ce dont il résulte que certains des abus de marché concernés par ce texte doivent être considérés comme des infractions graves (considérant 66).

38. En l'espèce, les informations privilégiées susceptibles de caractériser l'élément matériel de pratiques illicites en matière de marché étaient, par essence, orales et secrètes.

39. Se pose donc la question de savoir comment doit se concilier l'article 15§1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, avec les exigences posées par les dispositions précitées de la directive 2003/6 et du règlement 596/2014.

40. Pour répondre à une telle question, la jurisprudence existante ne parait pas fournir l'éclairage nécessaire dans ce cadre juridique et factuel inédit, de sorte qu'il n'est pas possible de dire que l'application correcte du droit de l'Union ne laisserait place à aucun doute raisonnable. Il convient en conséquence d'interroger la Cour de Justice.

41. Dans le cas où la réponse de la Cour de justice serait telle qu'elle conduirait la Cour de cassation à considérer que la législation française sur la conservation des données de connexion n'est pas conforme au droit de l'Union, il apparaît opportun de poser la question de savoir si les effets de cette législation pourraient être maintenus provisoirement afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment soient utilisées dans l'un des buts visés par cette législation.

42. Aussi convient-il de poser à la Cour de justice de l'Union européenne les questions préjudicielles suivantes mentionnées au dispositif.

II. Constitutionnalité de la disposition contestée

A. Normes de référence

1. Déclaration des droits de l'homme et du citoyen de 1789

- **Article 2**

Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression.

2. Constitution du 4 octobre 1958

- **Article 34**

La loi fixe les règles concernant :

- les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; les sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens ;

- la nationalité, l'état et la capacité des personnes, les régimes matrimoniaux, les successions et libéralités ;

- la détermination des crimes et délits ainsi que les peines qui leur sont applicables ; la procédure pénale ; l'amnistie ; la création de nouveaux ordres de juridiction et le statut des magistrats ;

- l'assiette, le taux et les modalités de recouvrement des impositions de toutes natures ; le régime d'émission de la monnaie.

(…)

La loi détermine les principes fondamentaux :

- de l'organisation générale de la défense nationale ;

- de la libre administration des collectivités territoriales, de leurs compétences et de leurs ressources ;

- de l'enseignement ;

- de la préservation de l'environnement ;

- du régime de la propriété, des droits réels et des obligations civiles et commerciales ;

- du droit du travail, du droit syndical et de la sécurité sociale.

(…)

B. Jurisprudence du Conseil constitutionnel sur le droit au respect de la vie privée

1. Sur le contrôle des fichiers et le traitement des données à caractère personnel

- **Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle**

. En ce qui concerne l'article 36 :

43. Considérant que l'article 36 modifie les articles L. 161-31 et L. 162-1-6 du code de la sécurité sociale relatifs au contenu et à l'utilisation d'une "carte électronique individuelle inter-régimes" ainsi qu'à sa délivrance à tout bénéficiaire de l'assurance maladie ;

44. Considérant que les requérants font grief à ce dispositif de porter atteinte au respect de la vie privée ; qu'ils font valoir que le système informatisé de transmission d'informations relatives à la santé des titulaires de la carte ne présente pas toutes les garanties et " comporte le risque d'être déjoué " ;

45. Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : " Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression. " ; que la liberté proclamée par cet article implique le respect de la vie privée ;

46. Considérant qu'aux termes du I de l'article L. 161-31 du code de la sécurité sociale, la carte électronique individuelle " doit permettre d'exprimer de manière précise l'accord du titulaire ou de son représentant légal pour faire apparaître les éléments nécessaires non seulement à la coordination des soins mais aussi à un suivi sanitaire " ; que le II du même article dispose : " Dans l'intérêt de la santé du patient, cette carte comporte un volet de santé… destiné à ne recevoir que les informations nécessaires aux interventions urgentes ainsi que les éléments permettant la continuité et la coordination des soins " ; qu'en vertu du I de l'article L.162-1-6 du code de la sécurité sociale, l'inscription, sur la carte, de ces informations est subordonnée dans tous les cas à l'accord du titulaire ou, s'agissant d'un mineur ou d'un majeur incapable, de son représentant légal ; que les personnes habilitées à donner cet accord peuvent, par ailleurs, " conditionner l'accès à une partie des informations contenues dans le volet de santé à l'utilisation d'un code secret qu'elles auront-elles-mêmes établi " ; que l'intéressé a accès au contenu du volet de santé par l'intermédiaire d'un professionnel de santé habilité ; qu'il dispose du droit de rectification, du droit d'obtenir la suppression de certaines mentions et du droit de s'opposer à ce que, en cas de modification du contenu du volet de santé, certaines informations soient mentionnées ; qu'en outre, il appartiendra à un décret en Conseil d'État, pris après avis public et motivé du Conseil national de l'Ordre des médecins et de la Commission nationale de l'informatique et des libertés, de fixer la nature des informations portées sur le volet de santé, les modalités d'identification des professionnels ayant inscrit des informations sur ce volet, ainsi que les conditions dans lesquelles, en fonction des types d'information, les professionnels de santé seront habilités à consulter, inscrire ou effacer les informations ; que la méconnaissance des règles permettant la communication d'informations figurant sur le volet de santé, ainsi que celle des règles relatives à la modification des informations, seront réprimées dans les conditions prévues par le VI de l'article L. 162-1-6 du code de la sécurité sociale ; que les sanctions pénales prévues par ces dernières dispositions s'appliqueront sans préjudice des dispositions de la section V du chapitre VI du titre II du livre deuxième du code pénal intitulée " Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques " ; qu'enfin, le législateur n'a pas entendu déroger aux dispositions de l'article 21 de la loi du 6 janvier 1978 susvisée relatives aux pouvoirs de surveillance et de contrôle de la Commission nationale de l'informatique et des libertés ;

47. Considérant que l'ensemble des garanties dont est assortie la mise en œuvre des dispositions de l'article 36 de la loi, au nombre desquelles il convient de ranger les caractéristiques assurant la sécurité du système, sont de nature à sauvegarder le respect de la vie privée ;

- **Décision n° 2003-467 DC du 13 mars 2003 - Loi pour la sécurité intérieure**

- Quant au respect de la vie privée :

21. Considérant que le I de l'article 21 prévoit que : " Les services de la police nationale et de la gendarmerie nationale peuvent mettre en oeuvre des applications automatisées d'informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'Etat, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs " ; qu'aux termes du II du même article : " Les traitements mentionnés au I peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au premier alinéa du I. - Ils peuvent également contenir des informations sur les victimes de ces infractions ; ces dernières peuvent toutefois s'opposer à ce que les informations nominatives les concernant soient conservées dans le fichier dès lors que l'auteur des faits a été définitivement condamné " ;

22. Considérant que le III de l'article 21 place le traitement des informations nominatives sous le contrôle du procureur de la République compétent ; que celui-ci peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ; que la rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande ; qu'en cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention ; que les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de

classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles ;

23. Considérant que le IV de l'article 21 définit strictement les personnes, autres que les magistrats judiciaires, habilitées, en raison de leurs attributions de police judiciaire, à utiliser les traitements en cause ; qu'en vertu du V du même article : " Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article. Il précise notamment la liste des contraventions mentionnées au I, la durée de conservation des informations enregistrées, les modalités d'habilitation des personnes mentionnées au IV ainsi que, le cas échéant, les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès " ;

24. Considérant que l'article 22 de la loi déférée, qui modifie l'article 39 de la loi du 6 janvier 1978 susvisée, fixe les conditions et modalités selon lesquelles les données nominatives contenues dans les fichiers intéressant en particulier la sécurité publique peuvent être communiquées aux personnes intéressées ;

25. Considérant que l'article 23 dresse limitativement la liste des décisions judiciaires au titre desquelles une personne peut être inscrite dans le fichier des personnes recherchées ;

26. Considérant, enfin, ainsi qu'il ressort des débats parlementaires, que la loi du 6 janvier 1978 susvisée, que le législateur n'a pas entendu écarter, s'appliquera aux traitements en cause ;

27. Considérant que l'ensemble de ces garanties est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ;

- Quant à l'utilisation des traitements à des fins administratives :

28. Considérant que l'article 25 ne permet la consultation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire que pour des finalités déterminées ;

29. Considérant qu'il s'agit, en premier lieu, " des décisions de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux " ; qu'en pareil cas, la consultation a pour but exclusif de vérifier que le comportement des intéressés n'est pas incompatible avec l'exercice des fonctions ou missions envisagées ; qu'elle s'effectue dans la stricte mesure exigée par la protection de la sécurité des personnes et par la défense des intérêts fondamentaux de la Nation ; qu'elle donne lieu à information des intéressés ; qu'un décret en Conseil d'Etat doit fixer la liste des enquêtes administratives qui, en application de l'article 25 de la loi déférée, pourront donner lieu à la consultation des traitements automatisés d'informations personnelles mentionnés à son article 21 ;

30. Considérant que la consultation est également prévue " pour l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux " ; qu'en pareil cas, la consultation est faite par des agents de la police et de la gendarmerie spécialement habilités à cet effet ou, dans des conditions déterminées par décret en Conseil d'Etat, par des personnels investis de missions de police administrative désignés selon les mêmes procédures ;

31. Considérant que la consultation est enfin permise pour " l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense " ; qu'en pareil cas, la consultation est effectuée par des agents de la police et de la gendarmerie nationale spécialement habilités à cet effet ;

32. Considérant qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées ;

33. Considérant qu'eu égard aux motifs qu'elle fixe pour ces consultations, comme aux restrictions et précautions dont elle les assortit, la loi déférée ne méconnaît par elle-même aucune des exigences constitutionnelles ci-dessus mentionnées ;

34. Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : " Aucune décision administrative ou privée impliquant une appréciation sur un

comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ;

35. Considérant, enfin, que ces dispositions ne portent pas par elles-mêmes atteinte aux droits des étrangers, lesquels ne comprennent aucun droit de caractère général et absolu d'acquérir la nationalité française ou de voir renouveler leur titre de séjour ; qu'elles ne sauraient en revanche être entendues comme remettant en cause l'acquisition de la nationalité française lorsque celle-ci est, en vertu de la loi, de plein droit, ni le renouvellement d'un titre de séjour lorsque celui-ci est, en vertu de la loi, de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale ;

- Quant au principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs :

36. Considérant que l'atténuation de la responsabilité pénale des mineurs en fonction de l'âge, comme la nécessité de rechercher leur relèvement éducatif et moral par des mesures adaptées à leur âge et à leur personnalité, prononcées par une juridiction spécialisée ou selon des procédures appropriées, ont été constamment reconnues par les lois de la République depuis le début du vingtième siècle ; que ces principes trouvent notamment leur expression dans la loi du 12 avril 1906 sur la majorité pénale des mineurs, la loi du 22 juillet 1912 sur les tribunaux pour enfants et l'ordonnance du 2 février 1945 sur l'enfance délinquante ;

37. Considérant que ce principe n'est pas méconnu du seul fait que les dispositions contestées ne comportent pas de limitation quant à l'âge des personnes sur lesquelles sont recueillies des informations dans les conditions prévues à l'article 21 de la loi déférée ;

38. Considérant toutefois qu'il appartiendra au décret prévu au V de l'article 21 de la loi déférée de déterminer une durée de conservation conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants ;

- **Décision n° 2011-625 DC du 10 mars 2011 - Loi d'orientation et de programmation pour la performance de la sécurité intérieure**

8. Considérant, en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en oeuvre de manière adéquate et proportionnée à cet objectif ;

9. Considérant que la création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude ; qu'elle est ainsi justifiée par un motif d'intérêt général ;

10. Considérant, toutefois, que, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ;

11. Considérant que, dans sa décision du 13 mars 2003 susvisée, le Conseil constitutionnel a déclaré l'article 21 ainsi que l'article 25 de la loi du 18 mars 2003 pour la sécurité intérieure conformes à la Constitution sous les réserves mentionnées aux considérants 26, 34, 35, 38 et 43 de sa décision ; qu'il a jugé que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux traitements en cause et que toute personne inscrite dans le fichier doit pouvoir exercer son droit d'accès et de rectification des données qui la concernent dans les conditions prévues par l'article 39 de cette loi ; que, lorsque ces données sont consultées dans le cadre d'enquêtes administratives, elles ne peuvent constituer qu'un élément de la décision prise par l'autorité administrative, sous le contrôle du juge ; que l'utilisation de ces données ne saurait permettre de remettre en cause l'acquisition de la nationalité française lorsque, en vertu de la loi, celle-ci est de plein droit ; qu'elle ne saurait pas davantage interdire le renouvellement d'un titre de séjour lorsque, en vertu de la loi, celui-ci est de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale ; qu'enfin, s'agissant

des mineurs, il appartient au décret de déterminer une durée de conservation conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants ;

12. Considérant que les modifications apportées aux dispositions de l'article 21 de la loi du 18 mars 2003 susvisées à l'occasion de leur introduction aux articles 230-6 à 230-11 du code de procédure pénale renforcent le contrôle de l'autorité judiciaire sur les données enregistrées dans les fichiers d'antécédents ; que l'article 230-8 du code de procédure pénale prévoit que le procureur de la République ou le magistrat chargé de suivre la mise en oeuvre et la mise à jour des traitements se prononce, dans un délai d'un mois, sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification ; que cet article prévoit également que toutes les données relatives à des personnes mises en cause et maintenues dans les fichiers d'antécédents en dépit d'une décision de relaxe, d'acquittement, de non-lieu ou de classement sans suite, quel qu'en soit le motif, font l'objet d'une mention qui interdit l'accès à ces données dans le cadre d'une enquête administrative ; que la différence de régime de conservation des données, qui résulte de la faculté donnée au procureur de la République d'ordonner l'effacement lorsque le classement sans suite de la procédure est motivé par une insuffisance de charges, est fondée sur l'absence d'intérêt de conserver, dans ce cas, de telles données dans le fichier ;

(…)

. En ce qui concerne l'article 14 :

67. Considérant que l'article 14 de la loi déférée insère dans le titre IV du livre Ier du code de procédure pénale un chapitre III consacré aux logiciels de rapprochement judiciaire et comprenant les articles 230-20 à 230-27 ; qu'aux termes de l'article 230-20 : « Afin de faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs, les services de la police nationale et de la gendarmerie nationale chargés d'une mission de police judiciaire peuvent mettre en oeuvre, sous le contrôle de l'autorité judiciaire, des logiciels destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires réunies par ces services au cours :

« 1° Des enquêtes préliminaires, des enquêtes de flagrance ou des investigations exécutées sur commission rogatoire ;

« 2° Des procédures de recherche des causes de la mort ou d'une disparition prévues par les articles 74 et 74-1 » ;

68. Considérant qu'aux termes de l'article 230-21 : « Les données exploitées par les logiciels faisant l'objet du présent chapitre ne peuvent provenir que des pièces et documents de procédure judiciaire déjà détenus par les services mentionnés à l'article 230 20.

« Lorsque sont exploitées des données pouvant faire indirectement apparaître l'identité des personnes, celle-ci ne peut apparaître qu'une fois les opérations de rapprochement effectuées, et uniquement pour celles de ces données qui sont effectivement entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel » ;

69. Considérant que la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le respect de la vie privée ; qu'il appartient au législateur compétent, en vertu de l'article 34 de la Constitution, pour fixer les règles concernant la procédure pénale, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés ;

70. Considérant que l'utilisation des logiciels de rapprochement judiciaire permet la mise en oeuvre de traitements de données à caractère personnel recueillies à l'occasion d'enquêtes judiciaires ouvertes pour toutes catégories d'infractions quelle que soit leur gravité ; qu'il appartient au législateur d'adopter les garanties de nature à assurer la conciliation entre les objectifs et principes constitutionnels précités en tenant compte de la généralité de l'application de ces logiciels ;

71. Considérant, en premier lieu, que les dispositions des articles 230-20 et suivants n'ont pas pour objet et ne sauraient avoir pour effet de permettre la mise en oeuvre d'un traitement général des données recueillies à l'occasion des diverses enquêtes mentionnées à l'article 230-20 ; que l'article 230-23 prévoit que, sans préjudice des pouvoirs de contrôle attribués à la Commission nationale de l'informatique et des libertés, le traitement de données à caractère personnel au moyen des logiciels de rapprochement judiciaire est opéré sous le contrôle du procureur de la République ou de la juridiction d'instruction compétent ; qu'ainsi, ces logiciels ne pourront conduire qu'à la mise en oeuvre, autorisée par ces autorités judiciaires, de traitements de données à caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations ;

72. Considérant, en second lieu, que le premier alinéa de l'article 230-22 dispose : « Les données à caractère personnel éventuellement révélées par l'exploitation des enquêtes et investigations mentionnées au 1° de l'article

230-20 sont effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans après le dernier acte d'enregistrement » ; qu'eu égard à la possibilité ouverte par les dispositions précitées d'un enregistrement de données même liées à des faits de faible gravité, la conservation de ces données ne saurait être prolongée à l'initiative de l'enquêteur au-delà de trois ans après leur enregistrement ; que, par suite, les mots : « après le dernier acte d'enregistrement » doivent être déclarés contraires à la Constitution ;

73. Considérant que, sous les réserves énoncées au considérant 71 et compte tenu de la déclaration d'inconstitutionnalité partielle portant sur l'article 230-22, les dispositions de l'article 14 ne méconnaissent pas les exigences constitutionnelles précitées ;

- **Décision n° 2012-652 DC du 22 mars 2012 - Loi relative à la protection de l'identité**

8. Considérant, en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ;

9. Considérant que la création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude ; qu'elle est ainsi justifiée par un motif d'intérêt général ;

10. Considérant, toutefois, que, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ;

11. Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; que, par suite, les articles 5 et 10 de la loi doivent être déclarés contraires à la Constitution ; qu'il en va de même, par voie de conséquence, du troisième alinéa de l'article 6, de l'article 7 et de la seconde phrase de l'article 8 ;

- **Décision n° 2013-684 DC du 29 décembre 2013 - Loi de finances rectificative pour 2013**

12. Considérant que les dispositions de l'article 10 ont notamment pour objet de renforcer, en particulier en matière d'assurance-vie, les obligations déclaratives des organismes d'assurance ; que ceux-ci seront ainsi tenus de déclarer à l'administration fiscale la souscription et le dénouement des contrats de capitalisation et autres contrats de même nature, en particulier des contrats d'assurance-vie, et chaque année, leur encours au 1er janvier de l'année de la déclaration ainsi que leur valeur de rachat ou le montant du capital garanti, y compris sous forme de rente, à cette date ; que sont exclus du champ des obligations annuelles de déclaration les contrats dont la valeur est inférieure à 7 500 euros ; que les déclarations s'effectueront dans les conditions et les délais fixés par un décret en Conseil d'État ; que les sanctions prévues à l'article 1736 du code général des impôts s'appliqueront aux organismes d'assurance qui méconnaîtraient leurs obligations déclaratives ; que les informations transmises sont à la seule destination de l'administration fiscale qui est tenue à l'obligation de secret dans les conditions prévues à l'article L. 103 du livre des procédures fiscales ;

13. Considérant, enfin, que si la mise en oeuvre des dispositions de l'article 10 doit conduire à la création d'un traitement de données à caractère personnel des informations ainsi recueillies, il ressort des débats parlementaires, qu'en adoptant ces dispositions, le législateur n'a pas entendu déroger aux garanties apportées par la loi du 6 janvier 1978 susvisée relatives notamment aux pouvoirs de la Commission nationale de l'informatique et des libertés, qui s'appliqueront aux traitements en cause ; que, par suite, il appartiendra aux autorités compétentes, dans le respect de ces garanties et sous le contrôle de la juridiction compétente, de s'assurer que la collecte, l'enregistrement, la

conservation, la consultation, la communication, la contestation et la rectification des données de ce fichier des contrats d'assurance-vie seront mis en oeuvre de manière adéquate et proportionnée à l'objectif poursuivi ;

14. Considérant qu'il résulte de ce qui précède qu'au regard de l'objectif d'intérêt général poursuivi, les dispositions de l'article 10 ne portent pas une atteinte disproportionnée au droit au respect de la vie privée ; que ces dispositions, qui ne méconnaissent aucune autre exigence constitutionnelle, doivent être déclarées conformes à la Constitution ;

- **Décision n° 2014-690 DC du 13 mars 2014 - Loi relative à la consommation**

. En ce qui concerne le grief tiré de l'atteinte au droit au respect de la vie privée :

51. Considérant que la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en oeuvre de manière adéquate et proportionnée à cet objectif ;

52. Considérant que la création d'un traitement de données à caractère personnel destiné à recenser les crédits à la consommation contractés par les personnes physiques pour leurs besoins non professionnels, les incidents de paiement caractérisés liés aux crédits souscrits par ces personnes ainsi que les informations relatives aux situations de surendettement et aux liquidations judiciaires vise à prévenir plus efficacement et plus précocement les situations de surendettement en fournissant aux établissements et organismes financiers des éléments leur permettant d'apprécier, au moment de l'octroi du prêt, la solvabilité des personnes physiques qui sollicitent un crédit ou se portent caution et en conséquence de mieux évaluer le risque ; que, par la création du registre national des crédits aux particuliers, le législateur a poursuivi un motif d'intérêt général de prévention des situations de surendettement ;

53. Considérant que les informations enregistrées dans le registre national des crédits aux particuliers sont énumérées par le paragraphe IV de l'article L. 333-10 du code de la consommation ; qu'y figureront des informations relatives à l'état civil de la personne qui a souscrit le crédit, à l'identification de l'établissement ou de l'organisme à l'origine de la déclaration, à l'identification, à la catégorie et aux caractéristiques du crédit, aux incidents de paiement caractérisés, aux situations de surendettement et aux liquidations judiciaires prononcées, à la date de mise à jour des données et au motif et à la date des consultations effectuées ; qu'en vertu des dispositions de l'article L. 333-11, les informations relatives aux crédits seront conservées pendant la durée d'exécution du contrat de crédit ; que celles relatives aux incidents de paiement seront conservées jusqu'au paiement intégral des sommes dues, sans que la durée de conservation de ces informations puisse excéder cinq ans à compter de la date d'enregistrement de l'incident de paiement ; que celles relatives aux situations de surendettement seront conservées pendant la durée de l'exécution du plan ou des mesures, sans que la durée de conservation des informations puisse excéder sept ans ; que celles relatives à la procédure de rétablissement personnel, à la procédure de liquidation judiciaire ou à un effacement partiel de dettes seront conservées jusqu'à l'expiration d'une période de cinq ans à compter de la date d'homologation ou de clôture de la procédure ; que le traitement de données à caractère personnel qui est créé est ainsi destiné à recueillir et à conserver pendant plusieurs années des données précises et détaillées relatives à un grand nombre de personnes physiques débitrices ;

54. Considérant que les dispositions de l'article L. 333-8 du code de la consommation prévoient une consultation obligatoire de ce registre par les établissements et organismes financiers « avant toute décision effective d'octroyer un crédit à la consommation » ainsi qu'« avant de proposer à l'emprunteur de reconduire un contrat de crédit renouvelable et dans le cadre de la vérification triennale de solvabilité de l'emprunteur » ; qu'elles autorisent une consultation de ce registre par les caisses de crédit municipal avant toute décision effective d'octroi d'un prêt sur gage corporel ainsi que par les établissements ou organismes financiers pour les personnes qui se portent caution à l'occasion de l'octroi d'un crédit à la consommation ; qu'elles autorisent également une consultation des seules informations de ce registre relatives aux incidents de paiement caractérisés, aux situations de surendettement et aux liquidations judiciaires par les établissements et organismes financiers « avant qu'ils ne formulent une offre » de prêt immobilier ou de prêt viager hypothécaire et qu'elles prévoient que ces informations peuvent également « être prises en compte par ces mêmes établissements et organismes dans leurs décisions d'attribution des moyens de paiement, ainsi que pour la gestion des risques liés aux crédits souscrits par leurs clients » ; qu'elles interdisent enfin que les informations contenues dans le registre puissent être consultées ou utilisées à d'autres fins que celles expressément prévues, sous peine des sanctions de l'article 226-21 du code pénal ; que la consultation du registre est par ailleurs ouverte, en vertu de l'article L. 333-9, aux commissions de surendettement dans l'exercice de leur mission de traitement des situations de surendettement ainsi qu'aux greffes des tribunaux compétents dans le cadre de la procédure de traitement des situations de surendettement ; que le registre peut ainsi être consulté à de très nombreuses reprises et dans des circonstances très diverses ;

55. Considérant que l'article L. 333-19 autorise les établissements et organismes financiers à utiliser les informations collectées lors de la consultation du registre dans des systèmes de traitement automatisé de données ;

56. Considérant que l'article L. 333-20 subordonne à une autorisation individuelle et une habilitation, selon des procédures spécifiques internes aux établissements et organismes financiers, la consultation du registre par les personnels des établissements et organismes financiers ; qu'en renvoyant à un décret en Conseil d'État les modalités d'application de cette autorisation, le législateur n'a pas limité le nombre de personnes employées par ces établissements et organismes susceptibles d'être autorisées à consulter le registre ;

57. Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre, les dispositions contestées portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; que, par suite, les dispositions de l'article 67 doivent être déclarées contraires à la Constitution ; qu'il en va de même, par voie de conséquence, des dispositions des articles 68 à 72, qui en sont inséparables ;

- **Décision n° 2016-591 QPC du 21 octobre 2016 - Mme Helen S. [Registre public des trusts]**

3. La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

4. Le registre public des trusts institué par le deuxième alinéa de l'article 1649 AB du code général des impôts recense tous les trusts, au sens de l'article 792-0 bis du même code, dont la déclaration est rendue obligatoire par les premier et cinquième alinéas du même article. Ces trusts sont ceux dont l'administrateur, le constituant ou au moins l'un des bénéficiaires a son domicile fiscal en France ou ceux qui comprennent un bien ou un droit qui y est situé. Pour chaque trust recensé, ce registre précise la date de sa constitution ainsi que les noms de son administrateur, de son constituant, et de ses bénéficiaires. Le quatrième alinéa de l'article 1649 AB renvoie à un décret en Conseil d'État le soin de préciser les modalités de consultation de ce registre public.

5. En favorisant, par les dispositions contestées, la transparence sur les trusts, le législateur a entendu éviter leur utilisation à des fins d'évasion fiscale et de blanchiment des capitaux. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales.

6. La mention, dans un registre accessible au public, des noms du constituant, des bénéficiaires et de l'administrateur d'un trust fournit des informations sur la manière dont une personne entend disposer de son patrimoine. Il en résulte une atteinte au droit au respect de la vie privée. Or, le législateur, qui n'a pas précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant accès aux données de ce registre, placé sous la responsabilité de l'administration fiscale. Dès lors, les dispositions contestées portent au droit au respect de la vie privée une atteinte manifestement disproportionnée au regard de l'objectif poursuivi. Par conséquent, sans qu'il soit besoin d'examiner les autres griefs, le deuxième alinéa de l'article 1649 AB du code général des impôts doit être déclaré contraire à la Constitution.

- **Décision n° 2016-745 DC du 26 janvier 2017 - Loi relative à l'égalité et à la citoyenneté**

– Sur certaines dispositions de l'article 78 :

22. L'article L. 411-10 du code de la construction et de l'habitation prévoit que le ministère chargé du logement tient un répertoire des logements locatifs sociaux et de leurs habitants, pour permettre l'élaboration et la mise en œuvre des politiques publiques de l'habitat.

23. Le c du 1° du paragraphe I de l'article 78 de la loi déférée complète cet article L. 411-10. Il prévoit que, pour alimenter ce répertoire, les bailleurs sociaux transmettent au ministère chargé du logement le numéro d'immatriculation au répertoire national d'identification des personnes physiques de chaque occupant majeur d'un logement locatif social.

24. Les sénateurs requérants soutiennent que ces dispositions portent une atteinte injustifiée au droit au respect de la vie privée des occupants de logements sociaux.

25. La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

26. En adoptant les dispositions contestées, le législateur a entendu que le ministère chargé du logement soit en mesure d'établir une cartographie de l'occupation socio-économique du parc de logements sociaux, afin d'améliorer la mise en œuvre de la politique en matière d'attribution de ces logements. Il a ainsi poursuivi un objectif d'intérêt général.

27. Si les collectivités territoriales et certains de leurs établissements publics peuvent obtenir du représentant de l'État dans la région les informations relatives aux logements situés sur leur territoire contenues dans le répertoire, c'est en vertu du huitième alinéa de l'article L. 411-10, à la condition que ces informations aient été préalablement rendues anonymes.

28. Par ailleurs, le législateur a prévu au 4° du paragraphe I de l'article 78 que l'exploitation des données du répertoire par le groupement d'intérêt public mentionné à l'article L. 441-2-1 du code de la construction et de l'habitation est réalisée de manière à rendre impossible l'identification des intéressés.

29. Il en résulte que le législateur a retenu des modalités de collecte, d'enregistrement, de conservation, et de communication du numéro d'immatriculation au répertoire national d'identification des personnes physiques adéquates et proportionnées à l'objectif poursuivi. Par conséquent, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté.

- **Décision n° 2017-752 DC du 8 septembre 2017 - Loi pour la confiance dans la vie politique**

– Sur d'autres dispositions :

81. L'article 9 modifie l'article 6 de la loi du 11 octobre 2013, le quatrième alinéa du paragraphe V de l'article L. 4122-8 du code de la défense ainsi que le quatrième alinéa du paragraphe V de l'article 25 quinquies de la loi du 13 juillet 1983 mentionnée ci-dessus, pour prévoir que la Haute autorité pour la transparence de la vie publique peut exercer directement le droit de communication de certains documents ou renseignement, reconnu à l'administration fiscale à la section I du chapitre II du titre II de la première partie du livre des procédures fiscales, afin de recueillir toutes informations utiles à l'accomplissement de sa mission de contrôle.

82. Au nombre des prérogatives de communication conférées par l'article 9 à la Haute autorité compte, par renvoi à l'article L. 96 G du livre des procédures fiscales, le droit de se faire communiquer les données de connexion détenues par les opérateurs de communications électroniques, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service. Le paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques prévoit que les données de connexion détenues par les opérateurs de communications électroniques « 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 ». Ces données « 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 ». En vertu du premier alinéa du paragraphe II de l'article 6 de la loi du 21 juin 2004 mentionnée ci-dessus, les fournisseurs d'accès et les hébergeurs « 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 ».

83. La communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée des personnes faisant l'objet du contrôle. Faute d'avoir assorti la procédure prévue par les dispositions en cause de garanties suffisantes, le législateur a porté une atteinte disproportionnée à ce droit.

84. Par conséquent, l'article 9 est contraire à la Constitution.

- **Décision n° 2017-637 QPC du 16 juin 2017 - Association nationale des supporters [Refus d'accès à une enceinte sportive et fichier d'exclusion]**

10. La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère

personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

11. Le troisième alinéa de l'article L. 332-1 du code du sport permet aux organisateurs de manifestations sportives à but lucratif d'établir un traitement automatisé de données à caractère personnel recensant les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations.

12. En autorisant l'établissement d'un tel fichier, le législateur a entendu renforcer la sécurité des manifestations sportives à but lucratif, en permettant à leurs organisateurs d'identifier les personnes susceptibles d'en compromettre la sécurité. Il a ainsi poursuivi un objectif d'intérêt général.

13. Il ressort du texte adopté et des débats parlementaires que, par ces dispositions, le législateur n'a pas entendu déroger aux garanties apportées par la loi du 6 janvier 1978 mentionnée ci-dessus relatives notamment aux pouvoirs de la Commission nationale de l'informatique et des libertés, qui s'appliquent aux traitements en cause.

14. Le fichier prévu par les dispositions contestées ne peut être établi que par les organisateurs de manifestations sportives à but lucratif. Il ne peut recenser que les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations. Il ne peut être employé à d'autres fins que l'identification desdites personnes en vue de leur refuser l'accès à des manifestations sportives à but lucratif. Il en résulte que le traitement de données prévu par les dispositions contestées est mis en œuvre de manière adéquate et proportionnée à l'objectif d'intérêt général poursuivi.

15. Par suite, les dispositions du troisième alinéa de l'article L. 332-1 du code du sport, qui ne méconnaissent ni le droit au respect de la vie privée, ni aucun autre droit ou liberté que la Constitution garantit, doivent être déclarées conformes à la Constitution.

- **Décision n° 2017-670 QPC du 27 octobre 2017 - M. Mikhail P. [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires]**

– Sur le fond :

7. La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

8. En application de l'article 230-6 du code de procédure pénale, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies au cours des enquêtes préliminaires ou de flagrance ou au cours des investigations exécutées sur commission rogatoire et concernant tout crime ou délit et certaines contraventions de la cinquième classe. En application du premier alinéa de l'article 230-7 du même code, ces traitements peuvent contenir des informations sur les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission de ces infractions.

9. En application des dispositions contestées, ces traitements sont opérés sous le contrôle du procureur de la République territorialement compétent. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien. Le procureur de la République peut également ordonner l'effacement des données personnelles en cas de décision de non-lieu ou de classement sans suite. En application de l'article 230-9 du code de procédure pénale, un magistrat est chargé de suivre la mise en œuvre et la mise à jour de ces traitements. Il dispose des mêmes pouvoirs d'effacement que le procureur de la République. Il résulte d'une jurisprudence constante qu'aucune personne mise en cause autre que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite ne peut obtenir, sur le fondement des dispositions contestées, l'effacement des données qui la concernent. En autorisant la création de traitements de données à caractère personnel recensant des antécédents judiciaires et l'accès à ces traitements par des autorités investies par la loi d'attributions de police judiciaire et par certains personnels investis de missions de police administrative, le législateur a entendu leur confier un outil d'aide à l'enquête judiciaire et à certaines enquêtes administratives. Il a ainsi poursuivi les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public.

10. Toutefois, en premier lieu, en prévoyant que les fichiers d'antécédents judiciaires peuvent contenir les informations recueillies au cours d'une enquête ou d'une instruction concernant une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer à la commission

de certaines infractions, le législateur a permis que figurent dans ce fichier des données particulièrement sensibles. Ainsi, l'article R. 40-26 du code de procédure pénale prévoit que peuvent être enregistrés les éléments d'état civil, la profession ou la situation familiale de la personne et une photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale.

11. En deuxième lieu, les fichiers d'antécédents judiciaires sont susceptibles de porter sur un grand nombre de personnes dans la mesure où y figurent des informations concernant toutes les personnes mises en cause pour un crime, un délit et certaines contraventions de la cinquième classe.

12. En troisième lieu, le législateur n'a pas fixé la durée maximum de conservation des informations enregistrées dans un fichier d'antécédents judiciaires. Ainsi, l'article R. 40-27 du code de procédure pénale prévoit qu'elles sont conservées pendant une durée comprise entre cinq ans et quarante ans selon l'âge de l'individu et la nature de l'infraction.

13. En dernier lieu, ces informations peuvent être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative.

14. Dès lors, en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée. Le premier alinéa de l'article 230-8 du code de procédure pénale doit donc être déclaré contraire à la Constitution.

- **Décision n° 2018-765 DC du 12 juin 2018 - Loi relative à la protection des données personnelles**

. En ce qui concerne les 2° et 3° de l'article 13 :

47. La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

48. En premier lieu, d'une part, en adoptant les dispositions du 2° de l'article 13, le législateur a entendu permettre la mise en œuvre de traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes par des personnes collaborant au service public de la justice, telles que des associations d'aide aux victimes ou d'accompagnement de personnes placées sous main de justice. D'autre part, en adoptant les dispositions du 3° du même article, le législateur a également entendu ouvrir cette faculté aux personnes victimes ou mises en cause dans une procédure pénale, afin de leur permettre de préparer ou de mettre en œuvre un recours en justice. Ce faisant, le législateur a poursuivi des objectifs d'intérêt général.

49. En second lieu, d'une part, en prévoyant qu'elles s'appliquent aux personnes morales de droit privé collaborant au service public de la justice appartenant à des catégories dont la liste est fixée par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, ainsi qu'aux personnes agissant soit en tant que victimes ou mises en cause soit pour le compte de ces dernières, les dispositions contestées circonscrivent suffisamment le champ des personnes ainsi autorisées à mettre en œuvre un traitement de données à caractère personnel en matière pénale.

50. D'autre part, la mise en œuvre de ces traitements ne peut être effectuée, dans le premier cas, que dans la mesure strictement nécessaire à la mission exercée par la personne collaborant au service public de la justice et, dans le second, que pour une durée strictement proportionnée aux finalités poursuivies par les personnes victimes ou mises en cause. Dans ce dernier cas, la communication à un tiers n'est possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite des mêmes finalités.

51. Enfin, la mise en œuvre de ces traitements de données est subordonnée au respect des garanties prévues par le règlement du 27 avril 2016, en particulier les conditions posées à ses articles 5 et 6, et à celles prévues par la loi du 6 janvier 1978.

52. Il résulte de ce qui précède que le législateur, qui n'était pas tenu de prévoir un dispositif d'autorisation préalable des traitements de données en cause, n'a pas méconnu le droit au respect de la vie privée. Il n'est pas davantage resté en deçà de sa compétence. Les griefs tirés de la méconnaissance de l'article 2 de la Déclaration de 1789 et de l'article 34 de la Constitution doivent ainsi être écartés.

53. Les mots « ainsi que les personnes morales de droit privé collaborant au service public de la justice et appartenant à des catégories dont la liste est fixée par décret en Conseil d'État, pris après avis motivé et publié de

la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission » figurant au 1° de l'article 9 de la loi du 6 janvier 1978 et les dispositions du 3° du même article, qui ne méconnaissent aucune autre exigence constitutionnelle, sont conformes à la Constitution.

(…)

. En ce qui concerne le grief tiré de la méconnaissance du droit au respect de la vie privée :

80. D'une part, en autorisant la création de traitements de données à caractère personnel recensant des antécédents judiciaires et l'accès à ces traitements par des autorités investies par la loi d'attributions de police judiciaire et par certains personnels investis de missions de police administrative, le législateur a entendu leur confier un outil d'aide à l'enquête judiciaire et à certaines enquêtes administratives. Il a ainsi poursuivi les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public.

81. D'autre part, figurent dans ce fichier des données particulièrement sensibles pouvant être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative. Par ailleurs, le législateur n'a pas fixé la durée maximum de conservation des informations enregistrées. Toutefois, d'une part, les dispositions contestées permettent à toute personne ayant bénéficié d'une décision définitive de relaxe, d'acquittement, de condamnation avec dispense de peine ou de mention au casier judiciaire, de non-lieu ou de classement sans suite, de demander sans délai l'effacement ou la rectification des données la concernant. D'autre part, en l'absence d'une telle décision, la personne peut demander l'effacement ou la rectification des données dès lors qu'il ne figure plus aucune mention de nature pénale dans le bulletin n° 2 de son casier judiciaire. Indépendamment des règles légales de retrait des mentions d'une condamnation au bulletin n° 2, le juge pénal peut exclure expressément une telle mention lorsqu'il prononce cette condamnation ou par jugement rendu postérieurement sur la requête du condamné. Enfin, la mention est supprimée en cas de réhabilitation acquise de plein droit ou de réhabilitation judiciaire.

82. Il résulte de ce qui précède que le grief tiré de la méconnaissance au droit au respect de la vie privée doit être écarté.

- **<u>Décision n° 2019-796 DC du 27 décembre 2019 - Loi de finances pour 2020</u>**

– Sur l'article 154 :

75. L'article 154 autorise, à titre expérimental et pour une durée de trois ans, les administrations fiscale et douanière à collecter et à exploiter de manière automatisée les contenus accessibles publiquement sur les sites internet de certains opérateurs de plateforme, aux fins de recherche de manquements et d'infractions en matière fiscale et douanière.

76. Les requérants soutiennent que cet article ne relève pas du domaine des lois de finances. Les auteurs des première et troisième saisines lui font également grief d'instaurer un dispositif de surveillance sur internet qui porterait une atteinte inconstitutionnelle au droit au respect de la vie privée, au droit à la protection des données personnelles et, dès lors qu'il conduirait les utilisateurs d'internet à s'autocensurer, à la liberté d'expression et de communication.

. En ce qui concerne la place de l'article 154 dans la loi de finances :

77. Selon l'article 34 de la Constitution : « Les lois de finances déterminent les ressources et les charges de l'État dans les conditions et sous les réserves prévues par une loi organique ». Le premier alinéa de son article 47 dispose : « Le Parlement vote les projets de loi de finances dans les conditions prévues par une loi organique ». La loi organique du 1er août 2001 détermine le contenu de la loi de finances. En particulier, le a du 7° du paragraphe II de son article 34 prévoit que la loi de finances de l'année peut, dans sa seconde partie, comporter « des dispositions relatives à l'assiette, au taux et aux modalités de recouvrement des impositions de toute nature qui n'affectent pas l'équilibre budgétaire ».

78. L'article 154 de la loi déférée vise, afin de lutter contre la fraude fiscale, à doter les administrations fiscale et douanière d'un nouveau dispositif de contrôle pour le recouvrement de l'impôt. Cet article a donc sa place dans une loi de finances.

. En ce qui concerne certaines dispositions de l'article 154 :

79. La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

80. Il appartient au législateur d'assurer la conciliation entre l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales et le droit au respect de la vie privée.

81. Aux termes de l'article 11 de la Déclaration de 1789 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ». En l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services.

82. En vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Sur ce fondement, il est loisible au législateur d'édicter des règles de nature à concilier la poursuite de l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales avec l'exercice du droit de libre communication et de la liberté de parler, écrire et imprimer. Toutefois, la liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés. Les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi.

83. Les dispositions contestées autorisent l'administration à recourir à des moyens informatisés et automatisés pour collecter et exploiter les contenus accessibles sur les sites internet des opérateurs de plateforme de mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service. Elles lui permettent ainsi, d'une part, de collecter de façon indifférenciée d'importants volumes de données, relatives à un grand nombre de personnes, publiées sur de tels sites et, d'autre part, d'exploiter ces données, en les agrégeant et en opérant des recoupements et des corrélations entre elles. Ce faisant, et même s'il s'agit de données rendues publiques par les personnes qu'elles concernent, les dispositions contestées portent atteinte au droit au respect de la vie privée. Dans la mesure où elles sont susceptibles de dissuader d'utiliser de tels services ou de conduire à en limiter l'utilisation, elles portent également atteinte à l'exercice de la liberté d'expression et de communication.

84. Toutefois, en premier lieu, en adoptant les dispositions contestées, le législateur a entendu renforcer les moyens de contrôle des administrations fiscale et douanière, en les dotant de dispositifs informatisés et automatisés d'exploration de données personnelles rendues publiques sur internet, aux fins de recherche et de poursuite de manquements et d'infractions en matière fiscale et douanière. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales.

85. En deuxième lieu, les traitements de données autorisés par les dispositions contestées peuvent être mis en œuvre, d'une part, pour les besoins de la recherche de certains manquements et de certaines infractions dont la commission est rendue possible ou favorisée par l'usage d'internet. Il en va ainsi du défaut ou du retard de production d'une déclaration fiscale en cas de découverte d'une activité occulte et de la fabrication, de la détention, de la vente ou du transport illicites de tabac, réprimés par les sanctions fiscales prévues au c du 1 de l'article 1728 et à l'article 1791 ter du code général des impôts. Il en va de même des infractions, punies par des sanctions pénales, prévues aux 3°, 8° et 10° de l'article 1810 du même code et aux articles 414, 414-2 et 415 du code des douanes, qui répriment certaines pratiques frauduleuses en matière d'alcool, de tabac et de métaux précieux et des délits douaniers sanctionnant la contrebande, l'importation et l'exportation de marchandises non déclarées, ainsi que le blanchiment de produits financiers provenant d'un délit douanier ou d'une infraction à la législation sur les stupéfiants.

86. D'autre part, ces traitements de données peuvent être mis en œuvre pour rechercher l'insuffisance de déclaration mentionnée à l'article 1729 du code général des impôts découlant d'un manquement aux règles de domiciliation fiscale fixées à l'article 4 B. Si la commission de ce manquement n'est pas rendue possible ou favorisée par l'usage d'internet, il résulte des travaux parlementaires que le législateur, qui a souhaité limiter le nombre de manquements susceptibles d'être recherchés, a entendu viser un des cas les plus graves de soustraction à l'impôt, qui peut être particulièrement difficile à déceler.

87. En troisième lieu, les données susceptibles d'être collectées et exploitées doivent répondre à deux conditions cumulatives. D'une part, il doit s'agir de contenus librement accessibles sur un service de communication au public en ligne d'une des plateformes précitées, à l'exclusion donc des contenus accessibles seulement après saisie d'un mot de passe ou après inscription sur le site en cause. D'autre part, ces contenus doivent être manifestement rendus publics par les utilisateurs de ces sites. Il en résulte que ne peuvent être collectés et exploités que les contenus se rapportant à la personne qui les a, délibérément, divulgués. En outre, les données sensibles au sens du paragraphe I de l'article 6 de la loi du 6 janvier 1978 mentionnée ci-dessus, c'est-à-dire celles qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques et biométriques et celles concernant la santé et

la vie ou l'orientation sexuelles, ne peuvent faire l'objet d'aucune exploitation à des fins de recherche de manquements ou d'infractions.

88. En quatrième lieu, d'une part, les traitements de données autorisés par les dispositions contestées ne peuvent comporter aucun système de reconnaissance faciale. D'autre part, ils ne peuvent être mis en œuvre que par des agents des administrations fiscale et douanière ayant au moins le grade de contrôleur et spécialement habilités. Seule la conception des outils de traitement des données, à l'exclusion de leur collecte, de leur traitement et de leur conservation, peut être confiée à un sous-traitant de l'administration. Enfin, les personnes concourant à la conception et à la mise en œuvre des traitements en cause sont tenues au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal et précisées à l'article L. 103 du livre des procédures fiscales et à l'article 59 bis du code des douanes.

89. En cinquième lieu, les données qui s'avèrent manifestement sans lien avec les manquements et infractions recherchés ou qui constituent des données sensibles sont détruites au plus tard dans les cinq jours suivant leur collecte, sans aucune autre exploitation possible de ces données pendant ce délai. Les autres données doivent être détruites dans les trente jours si elles ne sont pas de nature à concourir à la constatation des manquements ou infractions. Seules peuvent être conservées les données strictement nécessaires à une telle constatation, dans la limite d'une année ou, le cas échéant, jusqu'au terme de la procédure pénale, fiscale ou douanière dans le cadre de laquelle elles sont utilisées.

90. En sixième lieu, en application du sixième alinéa du paragraphe I de l'article 154, lorsque les traitements réalisés permettent d'établir qu'il existe des indices qu'une personne a pu commettre une des infractions ou un des manquements recherchés, les données collectées sont transmises au service compétent de l'administration pour corroboration et enrichissement. Il en résulte qu'aucune procédure pénale, fiscale ou douanière ne peut être engagée sans qu'ait été portée une appréciation individuelle de la situation de la personne par l'administration, qui ne peut alors se fonder exclusivement sur les résultats du traitement automatisé. En outre, en application du septième alinéa du même paragraphe I, les données collectées ne peuvent être opposées à la personne que dans le cadre d'une procédure de contrôle mentionnée au titre II du code des douanes ou au chapitre premier du titre II de la première partie du livre des procédures fiscales, dans le respect du principe du contradictoire et des droits de la défense.

91. En septième lieu, le traitement instauré par les dispositions contestées est mis en œuvre dans le respect de la loi du 6 janvier 1978, à l'exception du droit d'opposition prévu à son article 110. Ainsi, les personnes intéressées bénéficient, notamment, des garanties relatives à l'accès aux données, à la rectification et à l'effacement de ces données ainsi qu'à la limitation de leur traitement.

92. En dernier lieu, il résulte du dernier alinéa du paragraphe I de l'article 154 que la mise en œuvre des traitements de données, tant lors de leur création que lors de leur utilisation, doit être proportionnée aux finalités poursuivies. Il appartiendra notamment, à ce titre, au pouvoir réglementaire, sous le contrôle du juge, de veiller à ce que les algorithmes utilisés par ces traitements ne permettent de collecter, d'exploiter et de conserver que les données strictement nécessaires à ces finalités.

93. Il résulte de tout ce qui précède que, pour la recherche des manquements et infractions mentionnés ci-dessus, le législateur a, compte tenu de l'ensemble des conditions énoncées aux paragraphes précédents, assorti le dispositif critiqué de garanties propres à assurer, entre le droit au respect de la vie privée et l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales, une conciliation qui n'est pas déséquilibrée. Il en résulte également que l'atteinte à l'exercice de la liberté d'expression et de communication est nécessaire, adaptée et proportionnée aux objectifs poursuivis.

94. En revanche, les dispositions contestées permettent également la collecte et l'exploitation automatisées de données pour la recherche du manquement prévu au b du 1 de l'article 1728 du code général des impôts, qui sanctionne d'une majoration de 40 % le défaut ou le retard de production d'une déclaration fiscale dans les trente jours suivant la réception d'une mise en demeure. Or, dans une telle situation, l'administration, qui a mis en demeure le contribuable de produire sa déclaration, a déjà connaissance d'une infraction à la loi fiscale, sans avoir besoin de recourir au dispositif automatisé de collecte de données personnelles. Dès lors, en permettant la mise en œuvre d'un tel dispositif pour la simple recherche de ce manquement, les dispositions contestées portent au droit au respect de la vie privée et à la liberté d'expression et de communication une atteinte qui ne peut être regardée comme proportionnée au but poursuivi. Par suite, les mots « b et » figurant au premier alinéa du paragraphe I de l'article 154 sont contraires à la Constitution.

95. Le reste du paragraphe I de l'article 154 de la loi déférée, qui ne méconnaît aucune autre exigence constitutionnelle, est conforme à la Constitution.

96. Pour apprécier s'il convient de pérenniser le dispositif expérimental en cause au terme du délai de trois ans fixé par la loi, il appartiendra au législateur de tirer les conséquences de l'évaluation de ce dispositif et, en particulier, au regard des atteintes portées aux droits et libertés précités et du respect des garanties précitées, de

tenir compte de son efficacité dans la lutte contre la fraude et l'évasion fiscales. À la lumière de cette évaluation, la conformité à la Constitution de ce dispositif pourra alors de nouveau être examinée.

- **Décision n° 2019-797 QPC du 26 juillet 2019 - Unicef France et autres [Création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés]**

4. La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

5. Il appartient au législateur d'assurer la conciliation entre l'objectif de lutte contre l'immigration irrégulière qui participe de la sauvegarde de l'ordre public, objectif de valeur constitutionnelle, et le droit au respect de la vie privée.

6. Les dispositions contestées créent un traitement automatisé comportant les empreintes digitales et la photographie des ressortissants étrangers qui se déclarent mineurs privés temporairement ou définitivement de la protection de leur famille. Ces données peuvent être recueillies dès que l'étranger sollicite une protection en qualité de mineur. Dans un tel cas, la collecte, l'enregistrement et la conservation des empreintes digitales et de la photographie d'un étranger permet aux autorités chargées d'évaluer son âge de vérifier qu'une telle évaluation n'a pas déjà été conduite.

7. En premier lieu, ces dispositions n'ont ni pour objet ni pour effet de modifier les règles relatives à la détermination de l'âge d'un individu et aux protections attachées à la qualité de mineur, notamment celles interdisant les mesures d'éloignement et permettant de contester devant un juge l'évaluation réalisée. À cet égard, la majorité d'un individu ne saurait être déduite ni de son refus opposé au recueil de ses empreintes ni de la seule constatation, par une autorité chargée d'évaluer son âge, qu'il est déjà enregistré dans le fichier en cause ou dans un autre fichier alimenté par les données de celui-ci. Elles ne méconnaissent pas l'exigence constitutionnelle de protection de l'intérêt supérieur de l'enfant.

8. En second lieu, en évitant la réitération par des personnes majeures de demandes de protection qui ont déjà donné lieu à une décision de refus, le traitement automatisé mis en place par les dispositions contestées vise à faciliter l'action des autorités en charge de la protection des mineurs et à lutter contre l'entrée et le séjour irréguliers des étrangers en France. Ce faisant, et alors qu'aucune norme constitutionnelle ne s'oppose par principe à ce qu'un traitement automatisé poursuive plusieurs finalités, le législateur a, en adoptant les dispositions contestées, entendu mettre en œuvre l'exigence constitutionnelle de protection de l'intérêt supérieur de l'enfant et poursuivi l'objectif de valeur constitutionnelle de lutte contre l'immigration irrégulière.

9. Par ailleurs, les dispositions contestées prévoient le recueil, l'enregistrement et le traitement des empreintes digitales et de la photographie des ressortissants étrangers qui sollicitent le bénéfice des dispositifs de protection de l'enfance et excluent tout dispositif de reconnaissance faciale. Ainsi, les données recueillies sont celles nécessaires à l'identification de la personne et à la vérification de ce qu'elle n'a pas déjà fait l'objet d'une évaluation de son âge.

10. Enfin, d'une part, les dispositions contestées prévoient que la conservation des données des personnes reconnues mineures est limitée à la durée strictement nécessaire à leur prise en charge et à leur orientation, en tenant compte de leur situation personnelle. D'autre part, le fichier instauré par les dispositions contestées est mis en œuvre dans le respect de la loi du 6 janvier 1978 mentionnée ci-dessus.

11. Il résulte de ce qui précède que, en adoptant les dispositions contestées, le législateur a opéré entre la sauvegarde de l'ordre public et le droit au respect de la vie privée une conciliation qui n'est pas disproportionnée.

12. Par suite, l'article L. 611-6-1 du code de l'entrée et du séjour des étrangers et du droit d'asile, qui n'est pas entaché d'incompétence négative et ne méconnaît pas non plus le droit à un recours juridictionnel effectif ni aucun autre droit ou liberté que la Constitution garantit, doit être déclaré conforme à la Constitution.

- **Décision n° 2020-800 DC du 11 mai 2020 - Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions**

61. Il résulte du droit au respect de la vie privée que la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis

en œuvre de manière adéquate et proportionnée à cet objectif. Lorsque sont en cause des données à caractère personnel de nature médicale, une particulière vigilance doit être observée dans la conduite de ces opérations et la détermination de leurs modalités.

62. L'article 11 prévoit que, par dérogation à l'exigence fixée à l'article L. 1110-4 du code de la santé publique, les données à caractère personnel relatives à la santé des personnes atteintes par le covid-19 et des personnes en contact avec elles peuvent être traitées et partagées, sans le consentement des intéressés, dans le cadre d'un système d'information ad hoc ainsi que dans le cadre d'une adaptation des systèmes d'information relatifs aux données de santé déjà existants. La collecte, le traitement et le partage d'informations portent donc non seulement sur les données médicales personnelles des intéressés, mais aussi sur certains éléments d'identification et sur les contacts qu'ils ont noués avec d'autres personnes. Ce faisant, les dispositions contestées portent atteinte au droit au respect de la vie privée.

63. Toutefois, en premier lieu, en adoptant les dispositions contestées, le législateur a entendu renforcer les moyens de la lutte contre l'épidémie de covid-19, par l'identification des chaînes de contamination. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de protection de la santé.

64. Ensuite, la collecte, le traitement et le partage des données personnelles précitées ne peuvent être mis en œuvre que dans la mesure strictement nécessaire à l'une des quatre finalités suivantes : l'identification des personnes infectées par le covid-19, grâce à la prescription, la réalisation et la collecte des résultats des examens médicaux pertinents ainsi que la transmission des éléments probants de diagnostic clinique ; l'identification des personnes qui, ayant été en contact avec ces dernières, présentent un risque d'infection ; l'orientation des unes et des autres vers des prescriptions médicales d'isolement prophylactiques ainsi que leur accompagnement pendant et après la fin de ces mesures d'isolement ; la surveillance épidémiologique nationale et locale ainsi que la recherche sur le virus et les moyens de lutter contre sa propagation.

65. Enfin, le dispositif proposé exclut expressément le développement ou le déploiement d'une application informatique à destination du public et disponible sur équipement mobile permettant d'informer les personnes du fait qu'elles ont été à proximité de personnes diagnostiquées positives au covid-19.

66. En deuxième lieu, d'une part, le législateur a restreint le champ des données de santé à caractère personnel susceptibles de faire l'objet de la collecte, du traitement et du partage en cause, aux seules données relatives au statut virologique ou sérologique des personnes à l'égard du covid-19 ou aux éléments probants de diagnostic clinique et d'imagerie médicale précisés par décret en Conseil d'État. D'autre part, dans le cadre des trois premières finalités mentionnées ci-dessus, les autres données à caractère personnel en cause sont celles permettant l'identification des intéressés et celles précisant les contacts qu'une personne infectée a eus, au moment où elle a pu être infectée et pendant la période où elle était susceptible de contaminer d'autres personnes. Le législateur a ainsi restreint le champ des données à caractère personnel soumises au dispositif contesté aux seules données strictement nécessaires à la poursuite des trois premières finalités mentionnées ci-dessus.

67. Pour ce qui concerne la dernière finalité, relative à la surveillance épidémiologique et la recherche contre le virus, il est prévu que les nom et prénoms des intéressés, leur numéro d'inscription au répertoire national d'identification des personnes physiques et leur adresse soient supprimés. Sauf à méconnaître le droit au respect de la vie privée, cette exigence de suppression doit également s'étendre aux coordonnées de contact téléphonique ou électronique des intéressés.

68. En troisième lieu, peuvent avoir accès aux données enregistrées dans le système d'information le ministre de la santé, l'Agence nationale de santé publique, un organisme d'assurance maladie, les agences régionales de santé, le service de santé des armées, les communautés professionnelles territoriales de santé, les établissements de santé, sociaux et médico–sociaux, les équipes de soins primaires mentionnées à l'article L. 1411–11–1 du code de la santé publique, les maisons de santé, les centres de santé, les services de santé au travail mentionnés à l'article L. 4622–1 du code du travail et les médecins prenant en charge les personnes en cause, les pharmaciens, les dispositifs d'appui à la coordination des parcours de santé complexes prévus à l'article L. 6327–1 du code de la santé publique, les dispositifs spécifiques régionaux prévus à l'article L. 6327–6 du même code, les dispositifs d'appui existants qui ont vocation à les intégrer mentionnés au paragraphe II de l'article 23 de la loi du 24 juillet 2019 mentionnée ci-dessus, ainsi que les laboratoires et services autorisés à réaliser les examens de biologie ou d'imagerie médicale pertinents sur les personnes en cause.

69. Si le champ des personnes susceptibles d'avoir accès à ces données à caractère personnel, sans le consentement de l'intéressé, est particulièrement étendu, cette extension est rendue nécessaire par la masse des démarches à entreprendre pour organiser la collecte des informations nécessaires à la lutte contre le développement de l'épidémie.

70. En revanche, sont également inclus dans ce champ, pour le partage des données, les organismes qui assurent l'accompagnement social des intéressés. Or, s'agissant d'un accompagnement social, qui ne relève donc pas directement de la lutte contre l'épidémie, rien ne justifie que la communication des données à caractère personnel

traitées dans le système d'information ne soit pas subordonnée au recueil du consentement des intéressés. Dès lors, la deuxième phrase du paragraphe III de l'article 11, qui méconnaît le droit au respect de la vie privée, est contraire à la Constitution.

71. En outre, conformément au paragraphe III de l'article 11, chaque organisme n'est appelé à participer au système d'information mis en place que pour la part de ses missions susceptibles de répondre à l'une ou l'autre des finalités propres à ce système d'information et n'a accès qu'aux seules données nécessaires à son intervention. Il résulte également du paragraphe V du même article qu'un décret en Conseil d'État précisera, au sein de ces organismes, les services et personnels dont les interventions seraient, dans ce cadre, nécessaires, les catégories de données auxquelles ils auront accès, la durée de leurs accès ainsi que les règles de conservation de ces données.

72. Par ailleurs, conformément au sixième alinéa du paragraphe II de l'article 11, les agents de ces organismes ne sont pas autorisés à communiquer les données d'identification d'une personne infectée, sans son accord exprès, aux personnes qui ont été en contact avec elle. En outre, et de manière plus générale, ces agents sont soumis aux exigences du secret professionnel et ne peuvent donc, sous peine du délit prévu à l'article 226-13 du code pénal, divulguer à des tiers les informations dont ils ont connaissance par le biais du dispositif ainsi instauré.

73. Enfin, il appartiendra au pouvoir réglementaire de définir des modalités de collecte, de traitement et de partage des informations assurant leur stricte confidentialité et, notamment, l'habilitation spécifique des agents chargés, au sein de chaque organisme, de participer à la mise en œuvre du système d'information ainsi que la traçabilité des accès à ce système d'information.

74. En quatrième lieu, le paragraphe V de l'article 11 autorise les organismes précités à recourir, pour l'exercice de leur mission dans le cadre du dispositif examiné, à des organismes sous-traitants précisés par décret en Conseil d'État. Toutefois, d'une part, ces sous-traitants agissent pour leur compte et sous leur responsabilité. D'autre part, pour respecter le droit au respect de la vie privée, ce recours aux sous-traitants doit s'effectuer en conformité avec les exigences de nécessité et de confidentialité mentionnées aux paragraphes 71 à 73.

75. En cinquième lieu, si les dispositions contestées de l'article 11 exemptent la collecte, le traitement et le partage des données de santé de l'obligation d'obtenir le consentement des intéressés, elles n'exemptent pas ces mêmes opérations du respect des dispositions du règlement du 27 avril 2016 mentionné ci-dessus et de la loi du 6 janvier 1978 mentionnée ci-dessus relatives aux principes régissant les traitements des données à caractère personnel et aux droits reconnus aux personnes dont les données sont collectées, notamment leurs droits d'accès, d'information et de rectification.

76. En sixième lieu, d'une part, le dispositif instauré par l'article 11 ne peut s'appliquer au-delà du temps strictement nécessaire à la lutte contre la propagation de l'épidémie de covid-19 ou, au plus tard, au-delà de six mois après la fin de l'état d'urgence sanitaire déclaré par la loi du 23 mars 2020 mentionnée ci-dessus. D'autre part, les données à caractère personnel collectées, qu'elles soient ou non médicales, doivent, quant à elles, être supprimées trois mois après leur collecte.

77. En dernier lieu, le paragraphe V de l'article 11 prévoit que le décret d'application de la loi est pris après avis public conforme de la Commission nationale de l'informatique et des libertés. Or, en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Dès lors, le mot « conforme » figurant à la première phrase du paragraphe V de l'article 11 est contraire à la Constitution.

78. Il résulte de tout ce qui précède que, sous les réserves énoncées aux paragraphes 67, 73 et 74, les paragraphes I et II et le reste des paragraphes III et V de l'article 11 ne méconnaissent pas le droit au respect de la vie privée. Ces dispositions, qui ne sont pas non plus entachées d'incompétence négative ou inintelligibles ni ne méconnaissent d'autres exigences constitutionnelles, sont, sous les mêmes réserves, conformes à la Constitution.

- **<u>Décision n° 2021-819 DC du 31 mai 2021 - Loi relative à la gestion de la sortie de crise sanitaire</u>**

– Sur certaines dispositions de l'article 7 :

22. Le 1° du paragraphe I de l'article 7 de la loi déférée complète l'article 11 de la loi du 11 mai 2020 mentionnée ci-dessus par un paragraphe X afin de prévoir l'intégration au système national des données de santé des données recueillies dans le cadre des systèmes d'information mis en œuvre aux fins de lutter contre l'épidémie de covid-19.

23. Les députés requérants soutiennent que les dispositions contestées méconnaîtraient le droit au respect de la vie privée. En effet, selon eux, le transfert de ces données au sein du système national des données de santé emporte un allongement de la durée de leur conservation qui ne serait ni justifié ni proportionné. La protection de ces données médicales, particulièrement sensibles, ne serait en outre pas assurée par des garanties adéquates, dès

lors qu'elles sont traitées sous une forme qui n'est pas réellement anonyme et qu'elles sont susceptibles d'être mises à disposition d'un grand nombre de personnes.

24. La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif. Lorsque sont en cause des données à caractère personnel de nature médicale, une particulière vigilance doit être observée dans la conduite de ces opérations et la détermination de leurs modalités.

25. L'article 11 de la loi du 11 mai 2020 prévoit que, par dérogation à l'exigence fixée à l'article L. 1110-4 du code de la santé publique, aux seules fins de lutter contre la propagation de l'épidémie de covid-19, les données à caractère personnel relatives à la santé des personnes atteintes par ce virus et des personnes en contact avec elles peuvent être traitées et partagées, sans le consentement des intéressés, dans le cadre d'un système d'information ad hoc. Les données à caractère personnel ainsi collectées ne peuvent, en principe, être conservées à l'issue d'une durée de trois mois.

26. Les dispositions contestées prévoient que ces données sont rassemblées au sein du système national des données de santé prévu à l'article L. 1461-1 du code de la santé publique, lorsqu'elles relèvent de son champ, et précisent qu'elles sont soumises au chapitre Ier du titre VI du livre IV de la première partie du même code.

27. Ce faisant, les dispositions contestées permettent que ces données soient conservées pour une durée maximale de vingt ans après leur transfert et que les personnes mentionnées à l'article L. 1461-3 du code de la santé publique soient autorisées à y accéder. Elles portent donc atteinte au droit au respect de la vie privée.

28. Toutefois, en premier lieu, en adoptant ces dispositions, le législateur a entendu améliorer les connaissances sur le virus responsable de l'épidémie de covid-19, en particulier sur ses effets à long terme, et renforcer les moyens de lutte contre celle-ci. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de protection de la santé.

29. Ensuite, il résulte du paragraphe III de l'article L. 1461-1 du code de la santé publique que ces données peuvent être mises à disposition pour des finalités limitativement énumérées : l'information sur la santé et l'offre de soins, la définition, la mise en œuvre et l'évaluation des politiques de santé, la connaissance des dépenses de santé, l'information des professionnels et des établissements sur leurs activités, la surveillance, la veille et la sécurité sanitaires, ainsi que la recherche, les études, l'évaluation et l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

30. Enfin, le paragraphe V du même article interdit le traitement de ces données à des fins de promotion de médicaments ou de produits de santé ou à des fins d'exclusion de garanties de contrats d'assurance ou de modification de cotisations ou de primes d'assurance.

31. En deuxième lieu, en application de l'article L. 1461-4 du code de la santé publique, le système national des données de santé ne contient ni les noms et prénoms des personnes, ni leur numéro d'inscription au répertoire national d'identification des personnes physiques, ni leur adresse. S'agissant des données transférées en application des dispositions contestées, sauf à méconnaître le droit au respect de la vie privée, cette exclusion doit également s'étendre aux coordonnées de contact téléphonique ou électronique des intéressés.

32. En troisième lieu, en application de l'article L. 1461-3 du code de la santé publique, l'accès aux données rassemblées au sein du système national des données de santé en application des dispositions contestées est soumis, selon les cas, à une procédure de déclaration ou d'autorisation préalable auprès de la Commission nationale de l'informatique et des libertés. Ensuite, en application du 2° du paragraphe IV de l'article L. 1461-1 du même code, les personnes autorisées à accéder à ces données sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal. En outre, en application du 3° du paragraphe IV de l'article L. 1461-1 du code de la santé publique, l'accès aux données s'effectue dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et autres traitements. Enfin, en application de l'article L. 1461-2 du même code, les données qui font l'objet d'une mise à la disposition du public « sont traitées pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées y est impossible ».

33. En dernier lieu, il résulte du paragraphe II de l'article 7 de la loi déférée que les personnes dont les données médicales sont rassemblées et mises à disposition par le système national des données de santé en sont informées « sans délai et par tout moyen ». Ces personnes sont également informées « des conséquences juridiques qui en résultent, s'agissant notamment de la durée de conservation de ces données, des personnes qui y ont accès et des finalités en vue desquelles elles peuvent être traitées » et « du droit d'opposition dont elles disposent en application de l'article 74 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ». Cette information est délivrée individuellement aux personnes dont les données sont collectées à compter de l'entrée en vigueur de la loi déférée.

34. Il résulte de ce qui précède que, sous la réserve énoncée au paragraphe 31, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté. Par conséquent, le paragraphe X de l'article 11 de la loi du 11

mai 2020, qui ne méconnaît aucune autre exigence constitutionnelle, est, sous la même réserve, conforme à la Constitution.

- **Décision n° 2021-952 QPC du 3 décembre 2021 - M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]**

6. Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression ». La liberté proclamée par cet article implique le droit au respect de la vie privée.

7. En vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il lui incombe d'assurer la conciliation entre, d'une part, l'objectif de valeur constitutionnelle de recherche des auteurs d'infraction et, d'autre part, le droit au respect de la vie privée.

8. L'article 77-1-1 du code de procédure pénale permet au procureur de la République ou, sur son autorisation, à un officier ou à un agent de police judiciaire, dans le cadre d'une enquête préliminaire, de requérir, par tout moyen, des informations détenues par toute personne publique ou privée y compris celles issues d'un système informatique ou d'un traitement de données nominatives, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.

9. L'article 77-1-2 prévoit que, sur autorisation du procureur de la République, l'officier ou l'agent de police judiciaire peut requérir d'un organisme public ou de certaines personnes morales de droit privé, par voie télématique ou informatique, la mise à disposition d'informations non protégées par un secret prévu par la loi, contenues dans un système informatique ou un traitement de données nominatives.

10. En permettant de requérir des informations issues d'un système informatique ou d'un traitement de données nominatives, les dispositions contestées autorisent ainsi le procureur de la République et les officiers et agents de police judiciaire à se faire communiquer des données de connexion ou à y avoir accès.

11. D'une part, les données de connexion comportent notamment les données relatives à l'identification des personnes, à leur localisation et à leurs contacts téléphoniques et numériques ainsi qu'aux services de communication au public en ligne qu'elles consultent. Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée.

12. D'autre part, en application des dispositions contestées, la réquisition de ces données est autorisée dans le cadre d'une enquête préliminaire qui peut porter sur tout type d'infraction et qui n'est pas justifiée par l'urgence ni limitée dans le temps.

13. Si ces réquisitions sont soumises à l'autorisation du procureur de la République, magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, le législateur n'a assorti le recours aux réquisitions de données de connexion d'aucune autre garantie.

14. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la recherche des auteurs d'infractions.

2. Sur le contrôle en matière d'accès aux données de connexion

- **Décision n° 2001-457 DC du 27 décembre 2001 - Loi de finances rectificative pour 2001**

- SUR L'ARTICLE 62 :

4. Considérant que le II de l'article 62 est relatif au droit de communication dont dispose l'administration fiscale, pour l'exercice de sa mission de contrôle, sur les données conservées et traitées dans le cadre de l'article L. 32-3-1 du code des postes et télécommunications ; que les I et III du même article, qui constituent avec le II les éléments

inséparables d'un dispositif d'ensemble, sont relatifs aux droits analogues conférés à l'administration des douanes, d'une part, et aux enquêteurs de la Commission des opérations de bourse, d'autre part ;

5. Considérant que, selon les sénateurs requérants, ces droits de communication seraient " insuffisamment précisés et encadrés " ; que l'article 62 encourrait " de sérieuses réserves liées à la protection des libertés publiques " ; qu'en effet, il serait donné " aux agents concernés la possibilité de profiter d'une dérogation nouvelle aux règles d'effacement et de protection de l'anonymat des communications " ;

6. Considérant qu'il appartient au législateur d'assurer la conciliation entre, d'une part, l'exercice des libertés constitutionnellement garanties et, d'autre part, la prévention des atteintes à l'ordre public et la lutte contre la fraude fiscale qui constituent des objectifs de valeur constitutionnelle ;

7. Considérant que les dispositions critiquées ont pour seul objet de préciser les conditions dans lesquelles s'exerce, sur les données conservées et traitées par les opérateurs de télécommunication et par les prestataires désignés aux articles 43-7 et 43-8 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, le droit de communication général conféré par la législation en vigueur aux agents des douanes, à ceux de la direction générale des impôts et aux enquêteurs de la Commission des opérations de bourse ;

8. Considérant qu'aux termes mêmes de la disposition contestée, le droit d'accès qu'elle ouvre à de telles données, dont la divulgation serait de nature à porter atteinte à la vie privée, ne peut s'exercer que " dans le cadre de l'article L. 32-3-1 du code des postes et télécommunications " ; que cet article énonce avec précision la nature et les conditions de conservation et de communication de ces informations ; qu'il en résulte, notamment, que les données susceptibles d'être conservées et traitées " portent exclusivement sur l'identification des personnes utilisatrices de services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers " ; " qu'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 " ; " qu'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 " ; que, par ailleurs, le droit de communication créé par l'article 62 au profit des services d'enquêtes douanières, fiscales et boursières s'exerce dans le respect des autres prescriptions légales relatives à l'accomplissement de leurs missions ;

9. Considérant, par suite, que le législateur a mis en œuvre, en les conciliant, les exigences constitutionnelles ci-dessus rappelées ; que cette conciliation n'est entachée d'aucune erreur manifeste ; que le grief dirigé contre l'article 62 doit être rejeté ;

- **Décision n° 2015-478 QPC du 24 juillet 2015 - Association French Data Network et autres [Accès administratif aux données de connexion]**

11. Considérant, en premier lieu, d'une part, qu'en vertu de l'article L. 246-1 du code de la sécurité intérieure, la procédure de recueil des données de connexion sur réquisition administrative peut s'exercer 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 paragraphe I de l'article 6 de la loi du 21 juin 2004 susvisée ; que l'article L. 32 du code des postes et des communications électroniques définit dans son 1° les communications électroniques comme « les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » et dans son 15° l'opérateur comme « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques » ; que le paragraphe II de l'article L. 34-1 du même code prévoit son application aux opérateurs de communications électroniques, et notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, et aux personnes qui fournissent au public des services de communications électroniques, ainsi qu'aux personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; que les personnes mentionnées aux 1 et 2 du paragraphe I de l'article 6 de la loi du 21 juin 2004 sont celles dont l'activité est d'offrir un accès à des services de communication au public en ligne et celles 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 ;

12. Considérant, d'autre part, qu'en vertu du même article L. 246-1, peuvent être recueillis par l'autorité administrative les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes susmentionnées ; que, selon les dispositions du VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées 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 et 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 ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées sont celles 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 ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

13. Considérant, en second lieu, qu'il résulte de l'article L. 246-1 que les données de connexion requises sont transmises par les opérateurs aux autorités administratives compétentes ; que selon l'article L. 246-3, lorsque les données de connexion sont transmises en temps réel à l'autorité administrative, celles-ci ne peuvent être recueillies qu'après « sollicitation » de son réseau par l'opérateur ; que, par suite, les autorités administratives ne peuvent accéder directement au réseau des opérateurs dans le cadre de la procédure prévue aux articles L. 246-1 et L. 246-3 ;

14. Considérant qu'il résulte de ce qui précède que le grief tiré de ce que le législateur, en ne définissant pas précisément la procédure de réquisition administrative des données de connexion détenues et traitées par les opérateurs de communications électroniques, a méconnu l'étendue de sa compétence dans des conditions affectant le droit au respect de la vie privée, doit être écarté ;

- **Décision n° 2015-715 DC du 5 août 2015 - Loi pour la croissance, l'activité et l'égalité des chances économiques**

– SUR CERTAINES DISPOSITIONS DE L'ARTICLE 216 :

134. Considérant que le 2° de l'article 216 permet à l'Autorité de la concurrence d'obtenir la communication de données de connexion ;

135. Considérant que le 2° de l'article 216 insère, avant le dernier alinéa de l'article L. 450-3 du code de commerce, un nouvel alinéa permettant aux agents mentionnés à l'article L. 450-1 du même code de « se faire communiquer les données conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34-1 du code des postes et des communications électroniques et par les prestataires mentionnés 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 et en obtenir la copie » ;

136. Considérant que les députés requérants soutiennent que les dispositions contestées portent une atteinte manifestement disproportionnée au droit au respect de la vie privée dès lors, d'une part, que les agents de l'Autorité de la concurrence pourront obtenir des données de connexion pour les besoins d'une simple enquête et, d'autre part, que ces agents n'encourent aucune sanction en cas de divulgation des informations obtenues ; que, selon eux, en ne prévoyant pas l'intervention de l'autorité judiciaire pour autoriser la communication des données, le législateur a également porté atteinte à la garantie des droits et à l'article 66 de la Constitution ;

137. Considérant que la communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée ; que, si le législateur a réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par le 2° de l'article 216 d'aucune autre garantie ; qu'en particulier, le fait que les opérateurs et prestataires ne sont pas tenus de communiquer les données de connexion de leurs clients ne saurait constituer une garantie pour ces derniers ; que, dans ces conditions, le législateur n'a pas assorti la procédure prévue par le 2° de l'article 216 de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions ;

138. Considérant que le 2° de l'article 216 est contraire à la Constitution ;

- **Décision n° 2017-646/647 QPC du 21 juillet 2017 - M. Alexis K. et autre [Droit de communication aux enquêteurs de l'AMF des données de connexion]**

8. En application des dispositions contestées, les agents de l'Autorité des marchés financiers habilités à conduire les enquêtes qu'elle ordonne peuvent se faire communiquer les données de connexion détenues par les opérateurs de communications électroniques, les fournisseurs d'accès à un service de communication au public en ligne ou

les hébergeurs de contenu sur un tel service. Le paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques prévoit que les données de connexion détenues par les opérateurs de communications électroniques « 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 ». Ces données « 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 ». En vertu du premier alinéa du paragraphe II de l'article 6 de la loi du 21 juin 2004 mentionnée ci-dessus, les fournisseurs d'accès et les hébergeurs « 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 ».

9. La communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée. Si le législateur a réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données dans le cadre d'une enquête et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par les dispositions en cause d'aucune autre garantie. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions.

10. Par conséquent, la seconde phrase du premier alinéa de l'article L. 621-10 du code monétaire et financier doit par conséquent être déclarée contraire à la Constitution.

- **Décision n° 2018-764 QPC du 15 février 2019 - M. Paulo M. [Droit de communication aux agents des douanes des données de connexion]**

7. En application des dispositions contestées, les agents des douanes ayant au moins le grade de contrôleur peuvent se faire communiquer les données de connexion détenues par les opérateurs de communications électroniques, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service. Le paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques prévoit que les données de connexion détenues par les opérateurs de communications électroniques « 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 ». Ces données « 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 ». En vertu du premier alinéa du paragraphe II de l'article 6 de la loi du 21 juin 2004 mentionnée ci-dessus, les fournisseurs d'accès et les hébergeurs « 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 ».

8. La communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée. Si le législateur a réservé à certains agents des douanes soumis au respect du secret professionnel le pouvoir d'obtenir ces données dans le cadre d'opérations intéressant leur service et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par les dispositions en cause d'aucune autre garantie. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions.

9. Par conséquent, le i du 1° de l'article 65 du code des douanes doit être déclaré contraire à la Constitution.

- **Décision n° 2019-789 QPC du 14 juin 2019 - Mme Hanen S. [Droit de communication des organismes de sécurité sociale]**

. En ce qui concerne l'article L. 114-20 du code de la sécurité sociale :

8. Par le renvoi général qu'il opère, sous réserve de quelques exceptions, à la section I du chapitre II du titre II de la première partie du livre des procédures fiscales, l'article L. 114-20 du code de la sécurité sociale étend à certains agents des organismes de sécurité sociale le droit de communication de certains documents et informations reconnu à l'administration fiscale.

9. Il résulte en particulier de ce renvoi aux articles L. 83 et L. 85 du livre des procédures fiscales que ce droit de communication peut notamment s'exercer auprès des établissements bancaires afin d'obtenir d'eux, sans qu'ils puissent opposer le secret professionnel, les relevés de comptes et les autres documents bancaires relatifs au bénéficiaire d'une prestation sociale ou à son ayant droit ou à un cotisant. Il résulte également du renvoi opéré par les dispositions contestées aux articles L. 83 et L. 96 G du même livre que les agents des organismes de sécurité sociale disposent du droit de se faire communiquer les données de connexion détenues par les opérateurs de communications électroniques, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service. La communication de telles données est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée.

10. En premier lieu, en adoptant les dispositions contestées, le législateur a poursuivi l'objectif de valeur constitutionnelle de lutte contre la fraude en matière de protection sociale.

11. En deuxième lieu, d'une part, en vertu de l'article L. 114-19 du code de la sécurité sociale, il ne peut être fait usage du droit de communication que pour le contrôle de la sincérité et de l'exactitude des déclarations souscrites ou de l'authenticité des pièces produites en vue de l'attribution et du paiement des prestations servies par les organismes de sécurité sociale, pour l'exercice des missions de contrôle des cotisants aux régimes obligatoires de sécurité sociale et de lutte contre le travail dissimulé et pour le recouvrement de prestations versées indûment à des tiers.

12. D'autre part, ce droit de communication, qui n'est pas assorti d'un pouvoir d'exécution forcée, n'est ouvert qu'aux agents des organismes de sécurité sociale, lesquels sont soumis, dans l'utilisation de ces données, au secret professionnel.

13. En dernier lieu, la communication de données bancaires permet à titre principal aux organismes sociaux d'avoir connaissance des revenus, des dépenses et de la situation familiale de la personne objet de l'investigation. Elle présente un lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation.

14. Si ces données peuvent révéler des informations relatives aux circonstances dans lesquelles la personne a dépensé ou perçu ses revenus, l'atteinte ainsi portée au droit au respect de la vie privée n'est pas disproportionnée au regard de l'objectif poursuivi. Il résulte de ce qui précède que le législateur a assorti le droit de communication contesté de garanties propres à assurer, entre le respect de la vie privée et l'objectif de valeur constitutionnelle de lutte contre la fraude en matière de protection sociale, une conciliation qui n'est pas déséquilibrée.

15. En revanche, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Par ailleurs, elles ne présentent pas de lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre le droit au respect de la vie privée et la lutte contre la fraude en matière de protection sociale.

16. Par conséquent, l'article L. 114-20 du code de la sécurité sociale, qui concerne notamment les données bancaires et les données de connexion, doit être déclaré contraire à la Constitution.

- **Décision n° 2020-841 QPC du 20 mai 2020 - La Quadrature du Net et autres [Droit de communication à la Hadopi]**

. En ce qui concerne le droit de communication portant sur tous documents et les données de connexion :

14. Les troisième et quatrième alinéas de l'article L. 331-21 du code de la propriété intellectuelle et le mot « notamment » figurant au cinquième alinéa du même article confèrent aux agents de la Haute autorité le droit d'obtenir communication et copie de tous documents, quel qu'en soit le support, y compris les données de connexion détenues par les opérateurs de communication électronique.

15. L'exercice de ce droit répond aux mêmes fins et garanties que celles énoncées aux paragraphes 9 et 10. En outre, le troisième alinéa de l'article L. 331-21 subordonne son exercice aux nécessités de la procédure mise en œuvre par la commission de protection des droits.

16. Toutefois, d'une part, en faisant porter le droit de communication sur « tous documents, quel qu'en soit le support » et en ne précisant pas les personnes auprès desquelles il est susceptible de s'exercer, le législateur n'a ni limité le champ d'exercice de ce droit de communication ni garanti que les documents en faisant l'objet présentent un lien direct avec le manquement à l'obligation énoncée à l'article L. 336-3 du code de la propriété intellectuelle, qui justifie la procédure mise en œuvre par la commission de protection des droits.

17. D'autre part, ce droit de communication peut également s'exercer sur toutes les données de connexion détenues par les opérateurs de communication électronique. Or, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, de telles données fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Elles ne présentent pas non plus nécessairement de lien direct avec le manquement à l'obligation énoncée à l'article L. 336-3.

18. Il résulte de ce qui précède que, dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation qui ne soit pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif de sauvegarde de la propriété intellectuelle.

19. Par conséquent, et sans qu'il soit besoin de se prononcer sur l'autre grief, les troisième et quatrième alinéas de l'article L. 331-21 du code de la propriété intellectuelle ainsi que le mot « notamment » figurant au dernier alinéa du même article doivent être déclarés contraires à la Constitution.

- **Décision n° 2021-952 QPC du 3 décembre 2021 - M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]**

Voir ci-dessus